ALCATEL-LUCENT OmniSwitch 6850 Series

Technical Document

Table of Contents

OmniSwitch 6850 Series

Introduction

As Enterprises search for competitive advantages in the market place and become increasingly dependent on their networks to conduct business, new network requirements have rapidly emerged, exceeding the capabilities of successive technological advancements.

Enterprise new challenges include:

- Highly available, highly secure, highly intelligent, highly manageable and highly scalable Enterprise networks
- The rapid growth of Internet, Intranet and Extranet networking requirements
- Emerging new applications: converged IP applications, streaming media, desktop conferencing, IP-storage, etc.
- Increased clients (vendors, partners, customers, distributors, telecommuters, etc.) access to network resources
- Support high-density traffic aggregation in mission critical business network cores
- Today's Enterprise networks demanding higher switching capacities to improve performance and to accommodate higher 10GigE port densities. The trends in this market are mostly price driven.
  - 10GigE – Performance requirements
  - 10GigE – Port density requirements
- Various government requirements for IPv6
- Requirements for fast network response times

To meet these new market demands, the solution is to provide intelligent devices capable of supporting a host of advanced features for high volume intelligent traffic handling and processing. **Intelligent performance is essential.**
OmniSwitch 6850 Series value propositions, to support the Enterprise new challenges include:

- **Value**
- **High Availability**
- **Embedded Security**
- **Distributed Intelligence**
- **Simplified Manageability**

The OmniSwitch 6850 (OS6850) family is a new generation of stackable switching & routing platforms. 4.3.8
This AOS advanced switching & routing product family is considered as an evolution of the AOS OS6800 Series. The OmniSwitch 6850 platforms provide high availability, embedded security, distributed intelligence, easy-to-manage, high performance, and high throughput designed mainly for Enterprise Access and Distribution networks.
These features are available in a compact form factor at an extremely aggressive price point.

The OmniSwitch 6850 (OS6850) family is the Enterprise next generation stackable Switch / Router:

- A resilient, affordable & high performance solution
  - Large Gigabit Ethernet port density
  - 10 Gigabit Ethernet uplinks
  - Redundant architecture for converged networks
  - Native support for IPv4 & IPv6 for network future proofing
- A totally new Architecture
  - Extensive Multicast support (L2/IPv4/IPv6)
  - Enhanced network response time
  - Protecting the control plane from external attacks (DoS)

Power Options

The OS6850 family offers customers a vast selection of switches and power options that will accommodate most needs. By providing both 24- and 48-port PoE and non-PoE models with multiple power supply options such as AC and DC options as well as backup power supplies, network administrators can prevent over or under provisioning power to their switches and save money by not having to purchase more than they need.

The primary as well as the backup power supplies for the OS6850 models are external and connect to the rear of the unit. There is a power shelf provided with the unit, which slides into the rear of the chassis and is used to hold either one 510W power supply or two 360Ws, 126W ACs or 120W DC power supplies. This narrow shelf allows the switch to be placed in tight quarters. The power supplies can also be connected using a cable for shallow chassis applications. In this case, the same power shelf can be mounted in the rack using the mounting ears, which are removable in case the PS needs to be plugged into the rear of the chassis.
All of the OS6850 fixed chassis types support redundant, dual hot-swappable power supplies. For dual 510W configurations, the system will be a 2U form factor if you prefer to remote mount all power supplies.

OmniSwitch 6850-24

The OmniSwitch 6850-24 is a stackable edge/workgroup switch offering 20 unshared 10/100/1000Base-T ports, as well as four combo ports individually configurable to be 10/100/1000Base-T or 1000Base-X high speed connections.
The front panel of the OS6850-24 chassis contains the following major components:
• System status and slot indicator LEDs
• (20) unshared 10/100/1000Base-T ports
• (4) shared combo 10/100/1000Base-T ports
• (4) Combo SFP slots for 1000Base-X connections
• Console port (RJ-45)
• USB port (USB 2.0) **(Future Release)**

OmniSwitch 6850-24 Specifications

Total unshared 10/100/1000BASE-T ports per switch (ports 1-20)	20
Total shared 10/100/1000BASE-T “combo” ports per switch (ports 21-24)	4
Total shared 1000BASE-X “combo” ports per switch (ports 21-24)	4
Total 10/100/1000BASE-T ports per stack	192 (stack of eight switches)
Total combo SFP slots per stack	32 (stack of eight switches)
Power Supply	AC-to-DC 126W output P/S or DC-to-DC 120W output P/S
Flash Memory size	64MB
RAM Memory size	256MB SDRAM
Overall Width (rack-mount flanges included)	19 inches, approx.
Chassis Width (rack-mount flanges not included)	17.5 inches
Height	1.5 inch
Height (rack units)	1 RU
Chassis Depth	10.5 inches without power supplies installed 16.75 inches with power supplies installed.
Weight	14 lbs. (6.24 kg) without the power supply
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Operating Temperature	0 to 45 degrees Celsius
Storage Temperature	-20 to 70 degrees, Celsius

Altitude	Operating altitude: sea level at 40 degrees, Celsius and 10000 feet at 0 degrees, Celsius Storage altitude: sea level to 40000 feet
Standards supported	802.3z, 802.3ab, 1000BASE-T, IEEE 802.3u
Data rate (RJ-45 Ports)	10 or 100Mbps (full or half duplex) 1 Gigabit per second (full duplex)
Data rate (SFP ports)	1 Gigabit per second (full duplex)
Maximum frame size	9,216 bytes 4.1.7
Connections supported	10/100/1000BASE-T and 1000BASE-X
Cables supported	10BaseT: unshielded twisted-pair (UTP) 100BaseTX: unshielded twisted-pair (UTP), Category 5, EIA/TIA 568 or shielded twisted-pair (STP), Category 5, 100 ohm 1000BaseT: unshielded twisted-pair (UTP), Category 5e
Maximum cable distance	100 meters

OmniSwitch 6850-48

The OmniSwitch 6850-48 is a stackable edge/workgroup switch offering 44 unshared 10/100/1000Base-T ports, as well as four combo ports individually configurable to be 10/100/1000Base-T or 1000Base-X high speed connections.
The front panel of the OS6850-48 chassis contains the following major components:
• System status and slot indicator LEDs
• (44) unshared 10/100/1000Base-T ports
• (4) shared combo 10/100/1000Base-T ports
• (4) Combo SFP slots for 1000Base-X connections
• Console port (RJ-45)
• USB port (USB 2.0) **(Future Release)**

OmniSwitch 6850-48 Specifications

Total unshared 10/100/1000BASE-T ports per switch (ports 5-48)	44
Total shared 10/100/1000BASE-T “combo” ports per switch (ports 1-4)	4
Total shared 1000BASE-X “combo” ports per switch (ports 1-4)	4
Total 10/100/1000BASE-T ports per stack	384 (stack of eight switches)
Total combo SFP slots per stack	32 (stack of eight switches)
Power Supply	AC-to-DC 126W output P/S or DC-to-DC 120W output P/S
Flash Memory size	64MB
RAM Memory size	256MB SDRAM
Overall Width (rack-mount flanges included)	19 inches, approx.
Chassis Width (rack-mount flanges not included)	17.5 inches
Height	1.5 inch
Height (rack units)	1 RU
Chassis Depth	10.5 inches without power supplies installed 16.75 inches with power supplies installed.
Weight	14 lbs. (6.24 kg) without the power supply
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)

Operating Temperature	0 to 45 degrees Celsius
Storage Temperature	-20 to 70 degrees, Celsius
Altitude	Operating altitude: sea level at 40 degrees, Celsius and 10000 feet at 0 degrees, Celsius Storage altitude: sea level to 40000 feet
Standards supported	802.3z, 803.2ab, 1000BASE-T, IEEE 802.3u
Data rate (RJ-45 Ports)	10 or 100Mbps (full or half duplex) 1 Gigabit per second (full duplex)
Data rate (SFP ports)	1 Gigabit per second (full duplex)
Maximum frame size	9,216 bytes 4.1.7
Connections supported	10/100/1000BASE-T and 1000BASE-X
Cables supported	10BaseT: unshielded twisted-pair (UTP) 100BaseTX: unshielded twisted-pair (UTP), Category 5, EIA/TIA 568 or shielded twisted-pair (STP), Category 5, 100 ohm 1000BaseT: unshielded twisted-pair (UTP), Category 5e
Maximum cable distance	100 meters

OmniSwitch 6850-24X

The OmniSwitch 6850-24X is a stackable edge/workgroup switch offering 20 unshared 10/100/1000Base-T Power over ports, two (2) 10 Gigabit XFP slots, as well as four combo ports individually configurable to be 10/100/1000Base-T or 1000Base-X high speed connections.
The front panel of the OS6850-24X chassis contains the following major components:
• System status and slot indicator LEDs
• (20) unshared 10/100/1000Base-T ports
• (4) shared combo 10/100/1000Base-T ports
• (4) Combo SFP slots for 1000Base-X connections
• (2) 10 Gigabit XFP slots
• Console port (RJ-45)
• USB port (USB 2.0) **(Future Release)**

OmniSwitch 6850-24X Specifications

Total unshared 10/100/1000BASE-T ports per switch (ports 1-20)	20
Total shared 10/100/1000BASE-T “combo” ports per switch (ports 21-24)	4
Total shared 1000BASE-X “combo” ports per switch (ports 21-24)	4
Total XFP Slots (ports 25-26)	2
Total 10/100/1000BASE-T ports per stack	192 (stack of eight switches)
Total combo SFP slots per stack	32 (stack of eight switches)
Power Supply	AC-to-DC 126W output P/S or DC-to-DC 120W output P/S
Flash Memory size	64MB
RAM Memory size	256MB SDRAM
Overall Width (rack-mount flanges included)	19 inches, approx.
Chassis Width (rack-mount flanges not included)	17.5 inches
Height	1.5 inch
Height (rack units)	1 RU

Chassis Depth	10.5 inches without power supplies installed 16.75 inches with power supplies installed.
Weight	14 lbs. (6.24 kg) without the power supply
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Operating Temperature	0 to 45 degrees Celsius
Storage Temperature	-20 to 70 degrees, Celsius
Altitude	Operating altitude: sea level at 40 degrees, Celsius and 10000 feet at 0 degrees, Celsius Storage altitude: sea level to 40000 feet
Standards supported	802.3z, 803.2ab, 1000BASE-T, IEEE 802.3u
Data rate (RJ-45 Ports)	10 or 100Mbps (full or half duplex) 1 Gigabit per second (full duplex)
Data rate (SFP ports)	1 Gigabit per second (full duplex)
Data rate (XFP Ports)	10 Gigabit per second (full duplex)
Maximum frame size	9,216 bytes 4.1.7
Connections supported	10/100/1000BASE-T, 1000BASE-X, and 10GBASE-X
Cables supported	10BaseT: unshielded twisted-pair (UTP) 100BaseTX: unshielded twisted-pair (UTP), Category 5, EIA/TIA 568 or shielded twisted-pair (STP), Category 5, 100 ohm 1000BaseT: unshielded twisted-pair (UTP), Category 5e
Maximum cable distance	100 meters

OmniSwitch 6850-48X

The OmniSwitch 6850-48X is a stackable edge/workgroup switch offering 48 unshared 10/100/1000Base-T ports and two (2) 10 Gigabit XFP slots.
The front panel of the OS6850-48X chassis contains the following major components:
• System status and slot indicator LEDs
• (48) unshared 10/100/1000Base-T ports
• (2) 10 Gigabit XFP slots
• Console port (RJ-45)
• USB port (USB 2.0) **(Future Release)**

OmniSwitch 6850-48X Specifications

Total unshared 10/100/1000BASE-T ports per switch (ports 1-48)	48
Total XFP Slots (Ports 49-50)	2
Total 10/100/1000BASE-T ports per stack	384 (stack of eight switches)
Power Supply	AC-to-DC 126W output P/S or DC-to-DC 120W output P/S
Flash Memory size	64MB
RAM Memory size	256MB SDRAM
Overall Width (rack-mount flanges included)	19 inches, approx.
Chassis Width (rack-mount flanges not included)	17.5 inches
Height	1.5 inch
Height (rack units)	1 RU
Chassis Depth	10.5 inches without power supplies installed 16.75 inches with power supplies installed.

Weight	14 lbs. (6.24 kg) without the power supply
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Operating Temperature	0 to 45 degrees Celsius
Storage Temperature	-20 to 70 degrees, Celsius
Altitude	Operating altitude: sea level at 40 degrees, Celsius and 10000 feet at 0 degrees, Celsius Storage altitude: sea level to 40000 feet
Standards supported	802.3z, 802.3ab, 1000BASE-T, IEEE 802.3u
Data rate (RJ-45 Ports)	10 or 100Mbps (full or half duplex) 1 Gigabit per second (full duplex)
Data rate (XFP Ports)	10 Gigabits per second (full duplex0
Maximum frame size	9,216 bytes 4.1.7
Connections supported	10/100/1000BASE-T and 1000BASE-X
Cables supported	10BaseT: unshielded twisted-pair (UTP) 100BaseTX: unshielded twisted-pair (UTP), Category 5, EIA/TIA 568 or shielded twisted-pair (STP), Category 5, 100 ohm 1000BaseT: unshielded twisted-pair (UTP), Category 5e
Maximum cable distance	100 meters

OmniSwitch 6850-P24

The OmniSwitch 6850-P24 is a stackable edge/workgroup switch offering 20 unshared 10/100/1000Base-T Power over Ethernet (PoE) ports, as well as four combo ports individually configurable to be 10/100/1000 Base-T PoE or 1000 Base-X high speed connections.
The front panel of the OS6850-P24 chassis contains the following major components:
• System status and slot indicator LEDs
• (20) unshared 10/100/1000Base-T PoE ports
• (4) shared combo 10/100/1000Base-T PoE ports
• (4) Combo SFP slots for 1000Base-X connections
• Console port (RJ-45)
• USB port (USB 2.0) **(Future Release)**

OmniSwitch 6850-P24 Specifications

Total unshared 10/100/1000BASE-T PoE ports per switch (ports 1-20)	20
Total shared 10/100/1000BASE-T PoE “combo” ports per switch (ports 21-24)	4
Total shared 1000BASE-X “combo” ports per switch (ports 21-24)	4
Total 10/100/1000BASE-T ports per stack	192 (stack of eight switches)
Total combo SFP slots per stack	32 (stack of eight switches)
Power Supply	AC-to-DC 510W output P/S or AC-to-DC 360W output P/S
Flash Memory size	64MB
RAM Memory size	256MB SDRAM
Overall Width (rack-mount flanges included)	19 inches, approx.
Chassis Width (rack-mount flanges not included)	17.5 inches
Height	1.5 inch
Height (rack units)	1 RU

Chassis Depth	10.5 inches without power supplies installed 16.75 inches with power supplies installed.
Weight	14 lbs. (6.24 kg) without the power supply
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Operating Temperature	0 to 45 degrees Celsius
Storage Temperature	-20 to 70 degrees, Celsius
Altitude	Operating altitude: sea level at 40 degrees, Celsius and 10000 feet at 0 degrees, Celsius Storage altitude: sea level to 40000 feet
Standards supported	802.3z, 802.3ab, 1000BASE-T, IEEE 802.3u, IEEE 802.3af (DTE Power via MDI MIB); IAB RFCs 826 , 894
Data rate (RJ-45 Ports)	10 or 100Mbps (full or half duplex) 1 Gigabit per second (full duplex)
Data rate (SFP ports)	1 Gigabit per second (full duplex)
Maximum frame size	9,216 bytes **4.1.7**
Connections supported	10/100/1000BASE-T and 1000BASE-X IP- phones, Bluetooth Access Points, Internet cameras, and other devices requiring power over Ethernet
Cables supported	10BaseT: unshielded twisted-pair (UTP) 100BaseTX: unshielded twisted-pair (UTP), Category 5, EIA/TIA 568 or shielded twisted-pair (STP), Category 5, 100 ohm 1000BaseT: unshielded twisted-pair (UTP), Category 5e
Power supplied to port	Default 15.4watts per port Configurable from 3watts to 20watts per port Using the 360watts P/S, the maximum available PoE power is 230 watts. Using the 510watts P/S, the maximum available PoE power is 380watts.
Maximum cable distance (RJ-45 ports)	100 meters

OmniSwitch 6850-P48

The OmniSwitch 6850-P48 is a stackable edge/workgroup switch offering 44 unshared 10/100/1000Base-T Power over Ethernet (PoE) ports, as well as four combo ports individually configurable to be10/100/1000Base-T PoE or 1000Base-X high speed connections.
The front panel of the OS6850-P48 chassis contains the following major components:
• System status and slot indicator LEDs
• (44) unshared 10/100/1000Base-T PoE ports
• (4) shared combo 10/100/1000Base-T PoE ports
• (4) Combo SFP slots for 1000Base-X connections
• Console port (RJ-45)
• USB port (USB 2.0) **(Future Release)**

OmniSwitch 6850-P48 Specifications

Total unshared 10/100/1000BASE-T PoE ports per switch (ports 5-48)	44
Total shared 10/100/1000BASE-T PoE “combo” ports per switch (ports 1-4)	4

Total shared 1000BASE-X “combo” ports per switch (ports 1-4)	4
Total 10/100/1000BASE-T ports per stack	384 (stack of eight switches)
Total combo SFP slots per stack	32 (stack of eight switches)
Power Supply	AC-to-DC 510W output P/S or AC-to-DC 360W output P/S
Flash Memory size	64MB
RAM Memory size	256MB SDRAM
Overall Width (rack-mount flanges included)	19 inches, approx.
Chassis Width (rack-mount flanges not included)	17.5 inches
Height	1.5 inch
Height (rack units)	1 RU
Chassis Depth	10.5 inches without power supplies installed 16.75 inches with power supplies installed.
Weight	14 lbs. (6.24 kg) without the power supply
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Operating Temperature	0 to 45 degrees Celsius
Storage Temperature	-20 to 70 degrees, Celsius
Altitude	Operating altitude: sea level at 40 degrees, Celsius and 10000 feet at 0 degrees, Celsius Storage altitude: sea level to 40000 feet
Standards supported	802.3z, 802.3ab, 1000BASE-T, IEEE 802.3u, IEEE 802.3af (DTE Power via MDI MIB); IAB RFCs 826, 894
Data rate (RJ-45 Ports)	10 or 100Mbps (full or half duplex) 1 Gigabit per second (full duplex)
Data rate (SFP ports)	1 Gigabit per second (full duplex)
Maximum frame size	9,216 bytes 4.1.7
Connections supported	10/100/1000BASE-T and 1000BASE-X IP- phones, Bluetooth Access Points, Internet cameras, and other devices requiring power over Ethernet
Cables supported	10BaseT: unshielded twisted-pair (UTP) 100BaseTX: unshielded twisted-pair (UTP), Category 5, EIA/TIA 568 or shielded twisted-pair (STP), Category 5, 100 ohm 1000BaseT: unshielded twisted-pair (UTP), Category 5e
Power supplied to port	Default 15.4watts per port Configurable from 3watts to 20watts per port Using the 360watts P/S, the maximum available PoE power is 230 watts. Using the 510watts P/S, the maximum available PoE power is 380watts.
Maximum cable distance (RJ-45 ports)	100 meters

OmniSwitch 6850-P24X

The OmniSwitch 6850-P24X is a stackable edge/workgroup switch offering 20 unshared 10/100/1000Base-T Power over Ethernet (PoE) ports, two (2) 10 Gigabit XFP slots, as well as four combo ports individually configurable to be 10/100/1000Base-T PoE or 1000Base-X high-speed connections.
The front panel of the OS6850-P24X chassis contains the following major components:
• System status and slot indicator LEDs
• (20) unshared 10/100/1000Base-T PoE ports
• (4) shared combo 10/100/1000Base-T PoE ports

• (4) Combo SFP slots for 1000Base-X connections
• (2) 10 Gigabit XFP slots
• Console port (RJ-45)
• USB port (USB 2.0) **(Future Release)**

OmniSwitch 6850-P24X Specifications

Total unshared 10/100/1000BASE-T PoE ports per switch (ports 1-20)	20
Total shared 10/100/1000BASE-T PoE "combo" ports per switch (ports 21-24)	4
Total shared 1000BASE-X "combo" ports per switch (ports 21-24)	4
Total XFP Slots (Ports 25-26)	2
Total 10/100/1000BASE-T ports per stack	192 (stack of eight switches)
Total combo SFP slots per stack	32 (stack of eight switches)
Power Supply	AC-to-DC 510W output P/S or AC-to-DC 360W output P/S
Flash Memory size	64MB
RAM Memory size	256MB SDRAM
Overall Width (rack-mount flanges included)	19 inches, approx.
Chassis Width (rack-mount flanges not included)	17.5 inches
Height	1.5 inch
Height (rack units)	1 RU
Chassis Depth	10.5 inches without power supplies installed 16.75 inches with power supplies installed.
Weight	14 lbs. (6.24 kg) without the power supply
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Operating Temperature	0 to 45 degrees Celsius
Storage Temperature	-20 to 70 degrees, Celsius
Altitude	Operating altitude: sea level at 40 degrees, Celsius and 10000 feet at 0 degrees, Celsius Storage altitude: sea level to 40000 feet
Standards supported	802.3z, 802.3ab, 1000BASE-T, IEEE 802.3u, IEEE 802.3af (DTE Power via MDI MIB); IAB RFCs 826, 894
Data rate (RJ-45 Ports)	10 or 100Mbps (full or half duplex) 1 Gigabit per second (full duplex)
Data rate (SFP ports)	1 Gigabit per second (full duplex)
Data rate (XFP Ports)	10Gigabit per second (full duplex)
Maximum frame size	9,216 bytes **4.1.7**
Connections supported	10/100/1000BASE-T and 1000BASE-X IP- phones, Bluetooth Access Points, Internet cameras, and other devices requiring power over Ethernet
Cables supported	10BaseT: unshielded twisted-pair (UTP) 100BaseTX: unshielded twisted-pair (UTP), Category 5, EIA/TIA 568 or shielded twisted-pair (STP), Category 5, 100 ohm 1000BaseT: unshielded twisted-pair (UTP), Category 5e
Power supplied to port	Default 15.4watts per port Configurable from 3watts to 20watts per port Using the 360watts P/S, the maximum available PoE power

	is 230 watts. Using the 510watts P/S, the maximum available PoE power is 380watts.
Maximum cable distance (RJ-45 ports)	100 meters

OmniSwitch 6850-P48X

The OmniSwitch 6850-P48X is a stackable edge/workgroup switch offering 48 unshared 10/100/1000Base-T Power over Ethernet (PoE) ports and two (2) 10 Gigabit XFP slots.
The front panel of the OS6850-P48X chassis contains the following major components:
• System status and slot indicator LEDs
• (48) unshared 10/100/1000Base-T PoE ports
• (2) 10 Gigabit XFP slots
• Console port (RJ-45)
• USB port (USB 2.0) **(Future Release)**

OmniSwitch 6850-P48X Specifications

Total unshared 10/100/1000BASE-T PoE ports per switch (ports 5-48)	48
Total XFP Slots (Ports 49-50)	2
Total 10/100/1000BASE-T ports per stack	384 (stack of eight switches)
Power Supply	AC-to-DC 510W output P/S or AC-to-DC 360W output P/S
Flash Memory size	64MB
RAM Memory size	256MB SDRAM
Overall Width (rack-mount flanges included)	19 inches, approx.
Chassis Width (rack-mount flanges not included)	17.5 inches
Height	1.5 inch
Height (rack units)	1 RU
Chassis Depth	10.5 inches without power supplies installed 16.75 inches with power supplies installed.
Weight	14 lbs. (6.24 kg) without the power supply
Humidity	5% to 90% Relative Humidity (Operating) 0% to 95% Relative Humidity (Storage)
Operating Temperature	0 to 45 degrees Celsius
Storage Temperature	-20 to 70 degrees, Celsius
Altitude	Operating altitude: sea level at 40 degrees, Celsius and 10000 feet at 0 degrees, Celsius Storage altitude: sea level to 40000 feet
Standards supported	802.3z, 802.3ab, 1000BASE-T, IEEE 802.3u, IEEE 802.3af (DTE Power via MDI MIB); IAB RFCs 826, 894
Data rate (RJ-45 Ports)	10 or 100Mbps (full or half duplex) 1 Gigabit per second (full duplex)
Data rate (XFP ports)	10 Gigabit per second (full duplex)
Maximum frame size	9,216 bytes 4.1.7
Connections supported	10/100/1000BASE-T IP- phones, Bluetooth Access Points, Internet cameras, and other devices requiring power over Ethernet
Cables supported	10BaseT: unshielded twisted-pair (UTP) 100BaseTX: unshielded twisted-pair (UTP), Category 5,

	EIA/TIA 568 or shielded twisted-pair (STP), Category 5, 100 ohm 1000BaseT: unshielded twisted-pair (UTP), Category 5e
Power supplied to port	Default 15.4watts per port Configurable from 3watts to 20watts per port Using the 360watts P/S, the maximum available PoE power is 230 watts. Using the 510watts P/S, the maximum available PoE power is 380watts.
Maximum cable distance (RJ-45 ports)	100 meters

10 Gigabit Ethernet Ports

OmniSwitch 6850 Series 10 Gigabit Network Interfaces provide up to two 10000 Mbps (10Gbps) connections per chassis. In addition, they can be used in enterprise applications including backbone connections in networks where 10Gigabit Ethernet is used as the backbone media.
The following 10 Gbps XFP types are supported:
XFPs are fully hot swappable and are available for both short-reach and long-reach applications.

- 10G-XFP-LR
- 10G-XFP-SR

The 10G-XFP-LR is a long-reach 10 Gigabit optical transceiver that supports single mode fiber over 1310 nm wavelengths. The 10G-XFP-LR supports 10-micron fiber up to a maximum distance of 10 kilometers.
The 10G-XFP-SR is a short-reach 10 Gigabit optical transceiver that supports multimode fiber over 850 nm wavelengths. The 10G-XFP-SR supports 50/62.5 micron fiber up to a maximum distance of 300 meters (depending on the grade of fiber used).

Technical Specifications Overview

Technical Specifications Overview	
Number of XFP ports	2 x 10GBASE-X slots
Connector types	LC
Standards supported	IEEE 802.3ae 10-Gigabit Ethernet
Data rate	10 Gigabit per second (full duplex)
Maximum frame size	9,216 bytes; jumbo frames (1,500 to 9,216 bytes) **4.1.7**
MAC addresses supported	32000 per Network Interface (NI) module
Connections supported	10GBASE-S, and 10GBASE-L
Fiber optic cables supported	Multimode (62.5 and 50 micron) and single mode
Power Budget	10G-XFP-SR: 7.3 dB 10G-XFP-LR: 9.4 dB
Output optical power	10G-XFP-SR: -7.3 dBm (minimum) 10G-XFP-LR: -8.2 to 0.5 dBm
Input optical power	10G-XFP-SR: -9.9 to -1.0 dBm 10G-XFP-LR: -14.4 to 0.5 dBm
Cable distances	• 10G-XFP-SR: 300 m (high modal bandwidth fiber is required to reach 300 meters) • 10G-XFP-LR: 10 km *Note: Please note that distances are based on optimal conditions and may decrease depending on such factors as fiber diameter and quality.*

10Gbps Small Form Factor Pluggable (XFPs)

10Gbps Small Form Factor Pluggable (XFPs) is fiber-based optical transceivers for use with OmniSwitch 6850s Models designated with “X”. XFPs are fully hot swappable and are available for both short-reach and long-reach applications.
The following XFP types are available:

- 10G-XFP-LR
- 10G-XFP-SR

The 10G-XFP-LR is a long-reach 10-Gigabit optical transceiver that supports single mode fiber over 1310 nm wavelengths. The 10G-XFP-LR supports 10-micron fiber up to a maximum distance of 10 kilometers.
The 10G-XFP-SR is a short-reach 10-Gigabit optical transceiver that supports multimode fiber over 850 nm wavelengths. The 10G-XFP-SR supports 50/62.5 micron fiber up to a maximum distance of 300 meters (depending on the grade of fiber used).

Hardware Architecture	
MAC Address Table (L2 Unicast MAC addresses)	Up to 16 K (16,384) MAC Addresses is supported per system. **4.1.10**
IP Address Table Routes (RIB)	48K routing table
L3 IPv4 Host Entries (FIB)	8K
L3 IPv4 LPM Routes (FIB)	12K
L3 IPv6 Host Entries (FIB)	4K
L3 IPv6 LPM Routes (FIB)	6K
Hardware Tunnels/Trunks	128
Flows/ACLs	2K
Meters	2K
Counters	2K
Packet Buffer Size per system	2MB
CPU	Free-scale MPC8248 processor (400MHZ)
BUS	Hi-Gig (Hi-Gig+ capable) & 32-bit 66MHZ PCI BUS & I2C BUS
Memory	256MB of SDRAM SO-DIMM is default (upgradeable to 512MB)
Flash	Boot Flash: default 8MB upgradeable to 32MB File System Flash: default 64MB of Compact FLASH for O/S storage
USB Port **(Future Release)**	Philips ISP1761 USB2.0 port on the front panel
Main Switching Fabric ASIC	OS6850-48 & P48: BCM56504 XGS Switch & BCM56502 XGS Switch OS6850-48X & P48X: BCM56504 XGS Switch & BCM56504 XGS Switch OS6850-24 & P24: BCM56502 XGS Switch OS6850-24X & P24X: BCM56504 XGS Switch
10-Gigabit Ethernet Interface	10-Gigabit Ethernet XAUI interface OS6850-48X & P48X: BCM8704 OS6850-24X & P24X: BCM8704
PHY	OS6850-48 & P48: 5464SR & 5464R OS6850-48X & P48X: 5464R OS6850-24 & P24: 5464R & 5464SR OS6850-24X & P24X: 5464R & 5464SR
Connectors	XFP, SFP, and RJ45 connectors
Stacking	2 HI-Gig stacking ports supports up to 8 unit stacking topology
Console Port	RS-232 Console Port (RJ-45 connector). The console-protecting chip SEMTEC LCDA15C-6 is used along with the RJ45 connector.
POE /(Power over Ethernet) In-line Power	Support POE with full compliance of IEEE 802.3af
EEPROM	Board ID EEPROM Atmel 24C02 (on based-board)
Front Panel LED	Front Panel 7-segment LED display for stack ID
Temperature Sensor	Temperature Sensor National Semi-Conductor LM77 is supported
Thermal detection & Shutdown	Thermal detection and shutdown is supported.
Clock	Real Time Clock chip M41T11
Power Supply	Pluggable main AC-to-DC and DC-to-DC Power Supply Redundant Power Supply (RPS) AC-to-DC and DC-to-DC N+1 redundant Power Supplies are supported. Out of box SPS with selection for Mono 510W or dual 360W and RUP support
Fans	3 fans for the chassis with FAN failure detection. Additional fans built in the power supplies.
LEDS	Per port Link/Activity/PoE monitoring LED support System Power, BPS, and Diagnostic LED support LEDS: • LED Status on Front Panel o OK (Diag/OK/Fan fail/Temp fail) o PRI (Primary/Secondary) o PWR (Main Power Supply Status) o RPS (Redundant Power Supply Status) • Single LED with dual color is used for each Gig Ethernet Port (link/activity/POE) • Single LED is used for each 10Gig Ethernet Port • Single LED is used for the fiber SFP ports.

Performance	
Performance	
Raw Fabric Capacity	• OS6850-48: **92Gbps Full Duplex or 184Gbps aggregate** • OS6850-48X: **112Gbps Full Duplex or 224Gbps aggregate** • OS6850-P48: **92Gbps Full Duplex or 184Gbps aggregate** • OS6850-P48X: **112Gbps Full Duplex or 224Gbps aggregate** • OS6850-24: **44Gbps Full Duplex or 88Gbps aggregate** • OS6850-24X: **64Gbps Full Duplex or 128Gbps aggregate** • OS6850-P24: **44Gbps Full Duplex or 88Gbps aggregate** • OS6850-P24X: **64Gbps Full Duplex or 128Gbps aggregate** • OS6850-U24X: **64Gbps Full Duplex or 128Gbps aggregate** **4.3.1**
Stacking Capacity & Throughput	**Capacity:** **40 Gbps = 20Gbps FD (10Gbps FD "Stack-A" and 10Gbps FD "Stack-B")** **Throughput:** **4.3.9** **The Stacking (Stack "A" & Stack "B") supports 2 x 10-Gigabit Eth ports at wire-speed:** **2 * 14,880,952.3 pps = 29,761,904.6pps (approx: 29.8Mpps)**
Throughput Performance Or Forwarding Rate Per Stand-Alone Switch Assuming: ▪ All traffic is forwarded through The Switch Fabric ASIC ▪ And where applicable: o Including the 2-port 10GigE uplink module throughput o Stacking (Stack A & Stack B) throughput	**The 2-port 10-Gigabit Eth uplink supports 2 x 10-Gigabit Eth ports at wire-speed:** **2 * 14,880,952.3 pps = 29,761,904.6pps (approx: 29.8Mpps)** **The Stacking (Stack "A" & Stack "B") supports 2 x 10-Gigabit Eth ports at wire-speed:** **2 * 14,880,952.3 pps = 29,761,904.6pps (approx: 29.8Mpps)** **The 48 Gigabit Eth ports throughput at wire-speeds:** **48 * 1,488,095.23 pps = 71,428,571.04pps (approx: 71.4Mpps)** **The 24 Gigabit Eth ports throughput at wire-speeds:** **24 * 1,488,095.23 pps = 35,714,285.52pps (approx: 35.7Mpps)** **The OmniSwitch 6850-48 supports up to 48 Gigabit Eth ports at wire-speeds: 71.4Mpps** **The OmniSwitch 6850-48X supports up to 48 Gigabit Eth ports at wire-speeds +** **the 2-port 10-Gigabit Eth uplink: 71.4Mpps + 29.8Mpps = 101.2Mpps** **The OmniSwitch 6850-P48 supports up to 48 Gigabit Eth ports at wire-speeds: 71.4Mpps** **The OmniSwitch 6850-P48X supports up to 48 Gigabit Eth ports at wire-speeds +** **the 2-port 10-Gigabit Eth uplink: 71.4Mpps + 29.8Mpps = 101.2Mpps** **The OmniSwitch 6850-24 supports up to 24 Gigabit Eth ports at wire-speeds: 35.7Mpps** **The OmniSwitch 6850-24X supports up to 24 Gigabit Eth ports at wire-speeds +** **the 2-port 10-Gigabit Eth uplink: 35.7Mpps + 29.8Mpps = 65.5Mpps** **The OmniSwitch 6850-P24 supports up to 24 Gigabit Eth ports at wire-speeds: 35.7Mpps** **The OmniSwitch 6850-P24X supports up to 24 Gigabit Eth ports at wire-speeds +** **the 2-port 10-Gigabit Eth uplink: 35.7Mpps + 29.8Mpps = 65.5Mpps** **The OmniSwitch 6850-U24X supports up to 24 Gigabit Eth ports at wire-speeds + 4.3.4** **the 2-port 10-Gigabit Eth uplink: 35.7Mpps + 29.8Mpps = 65.5Mpps** **4.3.2**
Layer-2 & Layer-3 Forwarding Rate Per port	Wire-speed on 10Mbps port→ 14,880 pps with 64 Byte packets Wire-speed on 100Mbps port→ 148,809 pps with 64 Byte packets Wire-speed on Gigabit Ethernet port→ 1,488,095 pps with 64 Byte packets Wire-speed on 10-Gigabit Ethernet port→ 14,880,952 pps with 64 Byte packets *Note: Assuming that all traffic is forwarded through the Main Switch Fabric ASIC:* **The 2-port 10-Gigabit Ethernet uplink supports 2 x 10-Gigabit Eth. ports at wire-speed.** **The Stacking (Stack "A" & Stack "B") supports 2 x 10-Gigabit Eth ports at wire-speed.** **The OmniSwitch 6850-24 stand-alone supports up to 24 Gigabit Ethernet ports at wire-speed.** **The OmniSwitch 6850-P24 stand-alone supports up to 24 Gigabit Ethernet ports at wire-speed.** **The OmniSwitch 6850-48 stand-alone supports up to 48 Gigabit Ethernet ports at wire-speed.** **The OmniSwitch 6850-P48 stand-alone supports up to 48 Gigabit Ethernet ports at wire-speed.**

Management: Alcatel-Lucent OmniVista 3.0.0 or later releases support s the OS6850 platforms.	
Configuration Mode	Command Line Interface (CLI), Telnet/SSH for remote CLI access, Web-based (HTTP/HTTPS) and SNMPv1/v2c/v3 for complete NMS integration **4.1.3**
Management Access types	Serial Console port for local & remote (modem dial up) access (RJ45) Out-of-band Ethernet access (10/100/1000RJ45) In-band Ethernet access
System Maintenance	Port Mirroring (one-to-one, many-to-one) RMON (Remote Monitoring): Statistics, History, Alarm & Events, and sFlow Local & Remote logging (Syslog) **4.1.3** Detailed Statistics / Alarm / Debug information per process L3 OAM (ICMP Ping and Traceroute) NTP (Network Time Protocol) Internal flash (Compact Flash) to feature: • Working Directory • Certified Directory
System file Transfer	XModem and FTP (File Transfer Protocol) / SFTP (Secure FTP) / SCP **4.1.4**
Max number of users in local database	65
Max number of users in LDAP/RADIUS/ACE Server database (depends on server capabilities)	Greater than 1000
Max number of SNMP users (login)	50
Max number of simultaneous SNMPv3 requests	50
Max number of simultaneous HTTP sessions	4
Max number of simultaneous Telnet sessions	4
Max number of simultaneous FTP sessions	4
Max number of simultaneous SSH Telnet / FTP sessions	8
Max number of simultaneous User Login sessions	13
Max number of simultaneous Authentications sessions (A-VLAN, A-ACL with RADIUS)	30
Max number of authenticated ports	48
Port Disable	You can configure a “Port Disable” rule to administratively disable an interface when matching a policy rule. To make the interface operational again, the port must be unplugged/plugged back or disabled/enabled using “interfaces s/p admin down” and “interfaces s/p admin up”. Also, a SNMP trap will be sent when an interface goes down when matching a port disable rule.
SNMP Traps	A “pktDrop’ SNMP trap will be sent out to the SNMP station when a port goes down because of a user-port shutdown profile or a port disable rule.
Port Monitoring	The same unit cannot support both mirroring and monitoring configuration i.e. a user cannot have a port monitoring and a port mirroring session on the same unit Only one monitoring session at a time across the entire system Only the first 64 bytes of the packet can be monitored. Due to the port monitoring file size, the system can only store the first 2K packets (i.e. 140K/64 = 2187) Enabling the monitoring function affects the performance. As every single monitored packet is enqueued to the CPU, the Q-Dispatcher has to de-queue and look at each and every packet to determine if the destination is PMM (port monitoring module). The performance will be limited by the efficiency of Q-Dispatcher de-queuing speed and also the speed at which PMM can get the packets from Q-Dispatcher through IPC. Due to the performance limitations, monitoring wire rate traffic is not possible at this time. The packets coming to CPU are always tagged and undergo the same FFP modifications as mirroring Port Monitoring not supported on Link Agg.
Port Mirroring	The N-to-1 port mirroring allows the user to specify multiple numbers of ports, range of ports as mirrored source in a single command. However the maximum number of mirror source ports could be set to 24 for the current release. A user can mirror multiple 10GigE towards 1 port GigE. Of course if more than 1 GigE of traffic we don't expect one to mirror more that the port can deliver Aggregate ports are allowed to be mirrored on the physical ports. Mirroring on the logical link aggregated port ID is not supported. In mirroring, the packet coming out of mirroring port may be different from the ingress packet, based on the type of switching. For all types of mirroring, the mirrored packet carries the FFP (Fast Filtering Processor) modification, mirrored packet may get modified. To mirror port 1/1 to port 1/4, you can choose the following options: • In-port • Out-port • Bi-directional
Port Mapping	Port mapping feature is supported on both OS6800s & OS6850s. Following are the limitations for the feature

	8 sessions are supported per standalone switch and stack An aggregable port of a link aggregation group cannot be a mapped port and vice versa A mirrored port cannot be a mapped port and vice versa A mobile port cannot be configured as a network port of a mapping session
SCP (secure copy)	"SCP" command can be used to get/put the file from/to the server. Since OS6800/OS6850 does not have any SCP-daemon running on the switch, therefore this feature only works when OS6800/OS6850 works as a client instead of the server. This feature has been validated with SSH 4.0 on Solaris and Linux platforms. Since SSH 4.0 contains SCP, SFTP and SSH features, therefore the system allows the network administrator to create the local user database to specify all domain or family of features (i.e. the family of feature that a user can have access). When a user is being created, all allowed access need to be defined.
SFLOW	SFlow is a sampling technology embedded within switches/routers defined in RFC 3176. It provides the ability to monitor the traffic flows. It requires an sFlow Agent running in the Switch/Router and a sFlow collector which receives and analyses the monitored data. SFlow agent running on the OS6850, combines interface counters and traffic flow (packet) samples on all the configured interfaces into sFlow Datagrams that are sent across the network to an sFlow collector (3rd Party software). Packet sampling is done in hardware and is non-CPU intensive. Current release will not support IPv6 as Collector.
Interswitch Protocols **4.1.6**	Alcatel Interswitch Protocols (AIP) is used to discover adjacent switches and retain mobile port information across switches. The following protocols are supported: • Alcatel Mapping Adjacency Protocol (AMAP), which is used to discover the topology of OmniSwitches and OmniSwitch/Routers (Omni S/R). • Group Mobility Advertisement Protocol (GMAP), which is used to retain learned mobile port and protocol information. These protocols are independent of each other and perform separate functions. (Note: GMAP is not supported in AOSv6.1.1r01 Release) AMAP Overview The Alcatel Mapping Adjacency Protocol (AMAP) is used to discover the topology of OmniSwitches or Omni S/R(s) in a particular installation. Using this protocol, each switch determines which OmniSwitches or Omni S/R(s) is adjacent to it by sending and responding to Hello update packets. For the purposes of AMAP, adjacent switches are those that: Have a Spanning Tree path between them Do not have any switch between them on the Spanning Tree path that has AMAP enabled AMAP switch ports are either in the discovery transmission state, common transmission state, or passive reception state. Ports transition to these states depending on whether or not they receive Hello responses from adjacent switches. Note. All Hello packet transmissions are sent to a well-known MAC address (0020da:007004).
Software	
Capability Maturity Model (CMM)	Alcatel-Lucent's Software Engineering Institute (SEI) Capability Maturity Model (CMM) rating for software processes meets the Level-2 (CMM-level-2) requirements.
The Ethernet software	The Ethernet software is responsible for a variety of functions that support the Ethernet, Gigabit Ethernet and 10Gigabit Ethernet ports on OmniSwitch 6850 Series switches. These functions include diagnostics, software loading, initialization, and configuration of line parameters, gathering statistics, and responding to administrative requests from SNMP or CLI.

Operating Systems

Wind River's VxWorks multi-tasking O/S version 5.4 with a Kernel version 2.5. Alcatel-Lucent O/S – AOS (Alcatel-Lucent's Operating Systems).
O/S: AOS (Alcatel-Lucent Operating Systems) based – common to OS9000, OS8800, OS7000, OS6800
The AOS is uploaded onto the Flash memory. The advantage of this switch running the AOS is that it is managed using the same interface as with the rest of the Alcatel-Lucent AOS switching & routing platforms. The AOS on the OS6850 platforms provides support for the majority of the features of the larger modular platforms including layer-3 unicast routing using RIPv1&v2, VRRP, or OSPFv2. Group mobility and authenticated VLANs as well as QoS and ACL functionality are supported making the OS6850 a highly functional solution for the core of the network.

Software	
Each OmniSwitch 6850 Chassis is shipped with base software. All advanced features (with the exception of Advanced Routing Software) are also included in the base software.	
Authenticated Services Software	
OS-SW-SBR-N	"[ECCN 5D992] Authentication bundle for Windows w/MD5, RC4, MD4, DES. This bundle provides Funk Software's Steel-Belted Radius Enterprise Edition for Microsoft Windows and includes an one-year maintenance contract (maintenance releases, 7X24 phone support and e-service web access)."
OS-SW-SBR-S	"[ECCN 5D992] Authentication Bundle for Solaris w/MD5, RC4, MD4, DES. This bundle provides Funk Software's Steel-Belted Radius Enterprise Edition for Sun Solaris and includes an one-year maintenance contract (maintenance releases, 7X24 phone support and e-service web access)."
Advanced Routing Software	
OS6850-SW-AR	OS6850 Advanced Routing software. Includes support for OSPF, BGP, PIM-SM and DVMRP.

High Availability

The Alcatel-Lucent AOS OmniSwitch product family has been designed from its inception to provide carrier-class availability to meet the needs of mission-critical, IP Communications, and converged network environments. With the increasing importance of networks carrying voice and real-time applications, there is an increased need for availability that reaches across the network links and end user devices. Additionally, there is also the need for high availability in the areas of security and manageability, with intelligence and performance as integral parts of the network infrastructure to enable enterprises to achieve their availability goals. A very cost effective, highly available, highly scalable and highly re-configurable network will be achieved when the OS6850 is deployed in your LAN enterprise network. The following is only a highlight of the availability features supported by the OmniSwitch 6850 Series:

- Smart Continuous Switching: Hot Swap, Management Module Fail-over, Power Monitoring, Redundancy, and Stackability
- Redundancy support: redundant management, redundant fabric, and redundant power supply **4.3.3**
- Hot swappable & hot insertable support: switch modules, MiniGBICs, and redundant power supply
- IEEE 802.1w rapid recovery spanning tree allows sub-second fail-over to redundant link
- IEEE 802.1d spanning tree for loop free topology and link redundancy
- IEEE 802.1s multiple spanning tree and Alcatel-Lucent per-VLAN spanning tree (1x1)
- Fast forwarding mode on user ports to bypass 30 second delay for spanning tree
- Static and IEEE 802.3ad dynamic link aggregation that supports automatic configuration of link aggregates with other switches.
- Broadcast storm control
- Redundant 1: 1 power provided by the Backup Power Supplies
- Redundant 1: 1 PoE power provided by the **PoE** Power Supplies
- BPDU blocking – automatically shuts down switch ports being used as user ports if a spanning tree BPDU packet is seen. Prevents unauthorized spanning-tree enabled attached bridges from operating.

The Spanning Tree Algorithm and Protocol (STP)	The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. Based on the IEEE 802.1D standard, the Alcatel-Lucent STP implementation distributes the Spanning Tree load between the primary switch management and the rest of the NI Modules. This ensures a Spanning Tree that continues to respond to STP Bridge Protocol Data Units (BPDU) received on switch ports and port link up and down states in the event of a primary switch management fail over to a secondary (backup) switch management. In addition, the Alcatel-Lucent distributed implementation incorporates the following Spanning Tree features: • Configures a physical topology into a single Spanning Tree to ensure that there is only one data path between any two switches. • Supports fault tolerance within the network topology. The Spanning Tree is reconfigured in the event of a data path or bridge failure or when a new switch is added to the topology. • Supports two Spanning Tree operating modes: *flat* (single STP instance per switch) and *1x1* (single STP instance per VLAN). • Supports three Spanning Tree Algorithms: 802.1D (standard STP) and 802.1w (RSTP), and 802.1s (MSTP). • Allows 802.1Q tagged ports and link aggregate logical ports to participate in the calculation of the STP topology. • On the OmniSwitch 6850, the 802.1w Rapid Spanning Tree Algorithm and Protocol (RSTP) is the default protocol enabled for a VLAN. The Distributed Spanning Tree software is active on all switches by default. As a result, a loop-free network topology is automatically calculated based on default Spanning Tree switch, VLAN, and port parameter values. It is only necessary to configure Spanning Tree parameters to change how the topology is calculated and maintained. **Spanning Tree Specifications:** IEEE Standards supported: ▪ 802.1D–Media Access Control (MAC) Bridges ▪ 802.1w–Rapid Reconfiguration (802.1D Amendment 2) ▪ 802.1Q–Virtual Bridged Local Area Networks ▪ 802.1s–Multiple Spanning Trees (802.1Q Amendment 3) Spanning Tree Operating Modes supported: ▪ Flat mode - one spanning tree instance per switch ▪ 1x1 mode - one spanning tree instance per VLAN Spanning Tree Protocols supported: ▪ 802.1D Standard Spanning Tree Algorithm and Protocol (STP) ▪ 802.1w Rapid Spanning Tree Algorithm and Protocol (RSTP) ▪ 802.1s Multiple Spanning Tree Protocol (MSTP) Spanning Tree Port eligibility: ▪ Fixed ports (non-mobile) ▪ 802.1Q tagged ports ▪ Link aggregate of ports Maximum number of 1x1 Spanning Tree instances: 253 Number of Multiple Spanning Tree Instances (MSTI) supported: 16 MSTI, in addition to the Common and Internal Spanning Tree instance (also referred to as MSTI 0).

IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)	The Alcatel-Lucent Multiple Spanning Tree (MST) implementation provides support for the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). In addition to the 802.1D Spanning Tree Algorithm and Protocol (STP) and the 802.1w Rapid Spanning Tree Algorithm and Protocol (RSTP), MSTP also ensures that there is always only one data path between any two switches for a given Spanning Tree instance to prevent network loops. MSTP is an enhancement to the 802.1Q Common Spanning Tree (CST), which is provided when an Alcatel-Lucent switch is running in the flat Spanning Tree operating mode. The flat mode applies a single spanning tree instance across all VLAN port connections on a switch. MSTP allows the configuration of Multiple Spanning Tree Instances (MSTIs) in addition to the CST instance. Each MSTI is mapped to a set of VLANs. As a result, flat mode can support the forwarding of VLAN traffic over separate data paths. In addition to 802.1s MSTP support, the 802.1D STP and 802.1w RSTP are still available in either the flat or 1x1 mode. However, if using 802.1D or 802.1w in the flat mode, the single spanning tree instance per switch algorithm applies. **MST Specifications:** **IEEE Standards supported:** • 802.1D–Media Access Control (MAC) Bridges • 802.1w–Rapid Reconfiguration (802.1D Amendment 2) • 802.1Q–Virtual Bridged Local Area Networks • 802.1s–Multiple Spanning Trees (802.1Q Amendment 3) **Spanning Tree Operating Modes supported:** • Flat mode - one spanning tree instance per switch • 1x1 mode - one spanning tree instance per VLAN **Spanning Tree Protocols supported:** • 802.1D Standard Spanning Tree Algorithm and Protocol (STP) • 802.1w Rapid Spanning Tree Algorithm and Protocol (RSTP) • 802.1s Multiple Spanning Tree Algorithm and Protocol (MSTP) **Spanning Tree Port Eligibility:** • Fixed ports (non-mobile) • 802.1Q tagged ports • Link aggregate of ports **Number of 1x1 Spanning Tree instances supported:** 253 **Number of Multiple Spanning Tree Instances (MSTI) supported:** • 16 MSTI in addition to the Common and Internal Spanning • Tree instance (also referred to as MSTI 0). **CLI Command Prefix Recognition:** All Spanning Tree commands support prefix recognition.
Static (OmniChannel) Link Aggregation **4.3.7**	Alcatel-Lucent's link aggregation software allows you to configure the following two different types of link aggregation groups: • **Static (OmniChannel) link aggregate groups** • **IEEE 802.3ad Dynamic link aggregate groups** Static Link aggregation allows you to combine 2, 4, or 8, physical connections into large virtual connections known as link aggregation *group*s. You can create up to 32 link aggregation groups on a standalone switch. You can create Virtual LANs (VLANs), configure Quality of Service (QoS) conditions, 802.1Q framing, a other networking features on link aggregation groups because the switch's software treats these Virtual links just like physical links. Load balancing for Layer 2 non-IP packets is on a MAC address basis and for IP packets the balancing algorithm uses IP address as well. Ports must be the same speed within the same link aggregate group. Using link aggregation can provide the following benefits: • **Scalability:** You can configure up to 32 link aggregation groups that can consist of 2, 4, or 8 10Mbps, 100Mbps, 1Gbps, or 10Gbps Ethernet links in the switch. • **Reliability:** If one of the physical links in a link aggregate group goes down (unless it is the last one) the link aggregate group can still operate. • **Ease of Migration:** Link aggregation can ease the transition from a 100 Mbps Ethernet backbones to Gigabit Ethernet backbones. **Static Link Aggregation Specifications:** Maximum number of link aggregation groups per switch: 32 Number of Links per group supported: 2,4, or 8 Range for optional group name: 1 to 225 characters *Note:* Link aggregation traps include one that will send a trap when a single link in the aggregate group is down or cannot join the aggregate group.

Dynamic (IEEE 802.3ad) Link Aggregation	Alcatel-Lucent's link aggregation software allows you to configure two different types of link aggregation groups: • **Static link aggregate (OmniChannel) groups** • **Dynamic link aggregate groups** Dynamic Link aggregation allows you to combine 2, 4, or 8 physical connections into large virtual connections known as link aggregation *group*s. You can create up to 32 link aggregation groups on a standalone switch. You can create Virtual LANs (VLANs), configure Quality of Service (QoS) conditions, 802.1Q framing, and other networking features on link aggregation groups because switch software treats these virtual links just like physical links. Link aggregation groups are identified by unique MAC addresses, which are created by the switch but can be modified by the user at any time. Load balancing for Layer 2 non-IP packets is on a MAC address basis and for IP packets the balancing algorithm uses IP address as well. Ports *must* be the same speed within the same aggregate group. Using link aggregation can provide the following benefits: • **Scalability:** On OmniSwitch 6850 switches, you can configure up to 32 link-aggregation groups that can consist of 2, 4, or 8 10-Mbps, 100-Mbps, 1-Gbps, or 10-Gbps Ethernet links. • **Reliability:** If one of the physical links in a link aggregate group goes down (unless it is the last one) the link aggregate group can still operate. • **Ease of Migration:** Link aggregation can ease the transition from a 100 Mbps Ethernet backbones to Gigabit Ethernet backbones. **Dynamic (IEEE 802.3ad) Link Aggregation Specifications:** IEEE Specification supported: IEEE 802.3ad – Aggregation of Multiple Link Segments Maximum number of link aggregation groups per stand-alone OmniSwitch 6850 Series switches: 32 Number of Links per group supported: 2,4, or 8 Range for optional group name: 1 to 225 characters Group actor admin key: 0 to 65535 Group actor system priority: 0 to 65535 Group partner system priority: 0 to 65535 Group partner admin key: 0 to 65535 Port actor admin key: 0 to 65535 Port actor system priority: 0 to 255 Port partner admin key: 0 to 65535 Port partner admin system priority: 0 to 255 Port actor port: 0 to 65535 Port actor priority: 0 to 255 Port partner admin port: 0 to 65535 Port partner admin port priority: 0 to 255 CLI Command Prefix Recognition: All dynamic link aggregation configuration commands support prefix recognition. *Note:* Link aggregation traps include one that will send a trap when a single link in the aggregate group is down or cannot join the aggregate group.
Automatic Monitoring	Automatic monitoring refers to the switch's built-in sensors that automatically monitor operations. If an error is detected (e.g., over-threshold temperature), the switch immediately sends a trap to the user. The trap is displayed on the console in the form of a text error message. (In the case of an over-threshold temperature condition, the chassis displays an amber TEMP LED in addition to sending a trap.)
Monitoring the Chassis	OmniSwitch 6850 Series switches can be monitored and managed via the console port using Command Line Interface (CLI) commands. The switches can also be monitored and managed via the Ethernet ports using CLI commands, WebView (Alcatel-Lucent AOS web-based Element Manager), SNMPv3, and Alcatel-Lucent OmniVista NMS.
Using LEDs to Visually Monitor the Chassis	The front panel of OS6850 switches and NI Modules provides status LEDs that are useful in visually monitoring the status of NI modules. Front panel LEDs include: • Ethernet Port LEDs, and Slot Indicator LED • System Status LEDs
User-Driven Monitoring	User-driven hardware monitoring refers to CLI commands that are entered by the user in order to access the current status of hardware components. The user enters "show" commands that output information to the console. Monitoring information for chassis components such as the optional back up power supply, chassis temperature sensor, chassis fans…etc.

Embedded Security

Alcatel's AOS OmniSwitch product family provides organizations with easy, robust and optimal ways to control access to individual infrastructure components and to the individual resources resident on the network both internally and externally. Hence, information security for Internet, Intranet and Extranet applications will be supported through the incorporation of an advanced security feature set. The OmniSwitch 6850 supports a distributed security approach, enhanced emerging security technologies, and helps secure the LAN edge using proactive and reactive strategies.

The following is only a highlight of the advanced security features supported by the OmniSwitch 6850 Series:

- Support of Microsoft Network Access Protocol (NAP)
- IEEE 802.1x industry standard port based authentication challenges users with a password before allowing network access
  - 802.1x multi-client, multi-VLAN support for per-client authentication and VLAN assignment
  - IEEE 802.1x with group mobility
  - IEEE 802.1x with MAC based authentication, group mobility or "guest" VLAN support
  - MAC-based authentication for non-802.1x host
  - Alcatel Access Guardian support
- Port Mapping (Private VLANs)
- Authenticated VLAN that challenges users with username and password and supports dynamic VLAN access based on user
- Support for host integrity check and remediation VLAN
- Security through the implementation of OmniVista Quarantine Manager (OV2770-QM) With OneTouch Security automation
- PKI authentication for SSH access
- Learned Port Security or MAC address lockdown allows only known devices to have network access preventing unauthorized network device access
- RADIUS and LDAP admin authentication prevents unauthorized switch management
- Secure Shell (SSH), Secure Socket Layer (SSL) and SNMPv3 for encrypted remote management communication
- Access Control Lists (ACLs) to filter out unwanted traffic including denial of service attacks; Access control lists (ACLs) are per port, MAC SA/DA, IP SA/DA, TCP/ UDP port; Flow based filtering in hardware (L1-L4)
- Support for Access Control List Manager (ACLMAN)
- Supports Microsoft Network Access Policy (NAP) protocol
- Switch protocol security
  - MD5 for RIPv2, OSPFv2 and SNMPv3
  - SSH for secure CLI session with PKI support
  - SSL for secure HTTP session

Security Servers supported	LDAP, RADIUS, and ACE Server
Learned Port Security (LPS)	Learned Port Security (LPS) provides a mechanism for authorizing source learning of MAC addresses on 10/100 and Gigabit Ethernet ports. The only types of Ethernet ports that LPS does not support are link aggregate and tagged (trunked) link aggregate ports. Using LPS to control source MAC address learning provides the following benefits: • A configurable source learning time limit that applies to all LPS ports. • A configurable limit on the number of MAC addresses allowed on an LPS port. • Dynamic configuration of a list of authorized source MAC addresses. • Static configuration of a list of authorized source MAC addresses. • Two methods for handling unauthorized traffic: stopping all traffic on the port or only blocking traffic that violates LPS criteria. Configurable LPS parameters allow the user to restrict the source learning of host MAC addresses to: • A specific amount of time in which the switch allows source learning to occur on all LPS ports • A maximum number of learned MAC addresses allowed on the port. • A list of configured authorized source MAC addresses allowed on the port. Additional LPS functionality allows the user to specify how the LPS port handles unauthorized traffic. The following two options are available for this purpose: • Block only traffic that violates LPS port restrictions; authorized traffic is forwarded on the port. • Disable the LPS port when unauthorized traffic is received; all traffic is stopped and a port reset is required to return the port to normal operation. LPS functionality is supported on the following 10/100 and Gigabit Ethernet port types: • Fixed (non-mobile) • Mobile • 802.1Q tagged • Authenticated LPS has the following limitations: • You cannot configure 802.1x and LPS on the same ports. • You cannot configure LPS on 10 Gigabit ports. • You cannot configure LPS on link aggregate and 802.1Q tagged ports. **Learned Port Security Specifications:** Ports eligible for LPS: 10/100 and Gigabit Ethernet ports (fixed, mobile, 802.1Q tagged, and authenticated ports) Ports not eligible for LPS: Link aggregated ports and 802.1Q (trunked) link aggregated ports

	Minimum number of learned MAC addresses allowed per port: 1 Maximum number of learned MAC addresses allowed per port: 100 Maximum number of configurable MAC address ranges per LPS port: 1 Max number of learned MAC addresses per OS6850 switch (applies to all ports on the switch): 8K
IP directed broadcast	An IP directed broadcast is an IP datagram that has all zeroes or all 1's in the host portion of the destination IP address. The packet is sent to the broadcast address of a subnet to which the sender is not directly attached. Directed broadcasts are used in denial-of-service "smurf" attacks. In a smurf attack, a continuous stream of ping requests is sent from a falsified source address to a directed broadcast address, resulting in a large stream of replies, which can overload the host of the source address. By default, the switch drops directed broadcasts. Typically, directed broadcasts should not be enabled.
DOS Attacks	By default, the switch filters denial of service (DoS) attacks, which are security attacks aimed at devices that are available on a private network or the Internet. Some of these attacks aim at system bugs or vulnerability (for example, teardrop attacks), while other types of these types of attacks involve generating large volumes of traffic so that network service will be denied to legitimate network users (such as Pepsi attacks). These attacks include the following: • ICMP Ping of Death—Ping packets that exceed the largest IP datagram size (65535 bytes) are sent to a host and hang or crash the system. • SYN Attack—Floods a system with a series of TCP SYN packets, resulting in the host issuing SYN-ACK responses. The half open TCP connections can exhaust TCP resources, such that no other TCP connections are accepted. • Land Attack—Spoofed packets are sent with the SYN flag set to a host on any open port that is listening. The machine may hang or reboot in an attempt to respond. • Teardrop/Bonk/Boink attacks—Bonk / Boink / teardrop attacks generate IP fragments in a special way to exploit IP stack vulnerabilities. If the fragments overlap the way those attacks generate packets, an attack is recorded. Since teardrop, bonk and Boink all use the same IP fragmentation mechanism to attack, these are no distinction between detection of these attacks. The old IP fragments in the fragmentation queue are also reaped once the reassemble queue goes above certain size. • Pepsi Attack—The most common form of UDP flooding directed at harming networks. A Pepsi attack is an attack consisting of a large number of spoofed UDP packets aimed at diagnostic ports on network devices. This can cause network devices to use up a large amount of CPU time responding to these packets. The switch can be set to detect various types of port scans by monitoring for TCP or UDP packets sent to open or closed ports. Monitoring is done in the following manner: • Packet penalty values set: TCP and UDP packets destined for open or closed ports are assigned a penalty value. Each time a packet of this type is received, its assigned penalty value is added to a running total. This total is cumulative and includes all TCP and UDP packets destined for open or closed ports. • Port scan penalty value threshold: The switch is given a port scan penalty value threshold. This number is the maximum value the running penalty total can achieve before triggering an SNMP trap. • Decay value: A decay value is set. The running penalty total is divided by the decay value every minute. • Trap generation: If the total penalty value exceeds the set port scan penalty value threshold, a trap is generated to alert the administrator that a port scan may be in progress.
Security through the implementation of OmniVista Quarantine Manager (OV2770-QM) With OneTouch Security automation	The CrystalSec Security Framework has been expanded with the addition of two solutions - Host Integrity Check and Attack Containment - and two partnerships - Sygate and Fortinet. The Quarantine Manager Application enables the Network Administrator to quarantine devices to protect the network from attacks. When blocking any network traffic such as in Denial Of Service (DOS) attacks, the application works with an external Intrusion Prevention System (IPS) such as Fortinet, to send Syslog messages to the Quarantine Manager, and/or Alcatel AOS switches to send SNMP traps to the Quarantine Manager. The information includes the address that was blocked. Quarantine Manager then sends this information to the rest of the network by placing the address into to a "Quarantined" VLAN. Depending on the rule that is written for the event, the address can be immediately quarantined or placed into a Candidate List that can be reviewed by the Network Administrator.
Automatic log-out	Automatic log-out based on a pre-configured timer is supported: The switch supports the capability of configuring the inactivity timer for a CLI, HTTP (including WebView), or FTP interface. When the switch detects no user activity for this period of time, the user is logged off the switch.

Authenticated VLANs A-VLANs	Authenticated VLANs control user access to network resources based on VLAN assignment and a user login process; the process is sometimes called user authentication or Layer 2 Authentication. (Another type of security is device authentication, which is set up through the use of port-binding VLAN policies or static port assignment. The terms *authenticated VLANs* (A-VLANs) and *Layer 2 Authentication* is synonymous. Layer 2 Authentication is different from another feature in the switch called Authenticated Switch Access, which is used to grant individual users access to manage the switch. An authenticated network requires several components: **Authentication servers—**A RADIUS or LDAP server must be configured in the network. The server contains a database of user information that the switch checks whenever a user tries to authenticate through the switch. *(Note that the local user database on the switch may not be used for Layer 2 authentication*.). Backup servers may be configured for the authentication server. • **RADIUS or LDAP server:** Follow the manufacturer's instructions for your particular server. The external server may also be used for Authenticated Switch Access. • **RADIUS or LDAP client in the switch:** The switch must be set up to communicate with the RADIUS or LDAP server. **Authentication clients—**Authentication clients login through the switch to get access to A-VLANs. There are three types of clients: • **AV-Client.** This is an Alcatel-proprietary authentication client. The AV-Client does not require an IP address prior to authentication. The client software must be installed on the user's end station. • **Telnet client:** Any standard Telnet client can be used. An IP address is required prior to authentication. • **Web browser client:** Any standard Web browser can be used (Netscape or Internet Explorer). An IP address is required prior to authentication. **Authenticated VLANs—**At least one authenticated VLAN must be configured. **Authentication port—**At least one mobile port must be configured on the switch as an authentication port. This is the physical port through which authentication clients are attached to the switch. **DHCP Server—**A DHCP server can provide IP addresses to clients prior to authentication. After authentication, any client can obtain an IP address in an authenticated VLAN to which the client is allowed access. A relay to the server must be set up on the switch. **Authentication agent in the switch—**Authentication is enabled when the server(s) and the server authority mode is specified on the switch. *Note:* AVLAN Web Authentication: The Mac OS X 10.3.x is supported for AVLAN web authentication using JVM-v1.4.2. The maximum number of possible A-VLAN users support is 2,048.
IEEE 802.1X *Note: there is no switch based local database for IEEE 802.1x authentication.* Here are the limits: Maximum number of supplicants / non-supplicant users per system: 1024 Maximum number of non-supplicant users per port: 1024 Maximum number of supplicant users per port: 253 Maximum combined number of supplicant and non-supplicant users per port: 1024 The system supports up to 1024 authenticated/mobile mac-addresses. The system can roughly processes ~200 mac per seconds.	Physical devices attached to a LAN port on the switch through a point-to-point LAN connection may be authenticated through the switch through port-based network access control. This control is available through the IEEE 802.1X standard implemented on the switch. In addition, Interoperability between Alcatel 802.1x and Sygate Management Server (SMS) and Sygate Enforcer is also supported. The identity field in Alcatel 802.1x authentication works with all applications that send more than 32 bytes (e.g., Sygate). **IEEE 802.1X Specifications:** RFCs Supported: ▪ RFC 2284–PPP Extensible Authentication Protocol (EAP) ▪ RFC 2865–Remote Authentication Dial In User Service (RADIUS) ▪ RFC 2866–RADIUS Accounting ▪ RFC 2867–RADIUS Accounting Modifications for Tunnel Protocol Support ▪ RFC 2868–RADIUS Attributes for Tunnel Protocol Sup-port ▪ RFC 2869–RADIUS Extensions IEEE Standards Supported: ▪ IEEE 802.1X-2001–Standard for Port-based Network Access Control ▪ 802.1X RADIUS Usage Guidelines The 802.1X standard defines port-based network access controls, and provides the structure for authenticating physical devices attached to a LAN. It uses the Extensible Authentication Protocol over LAN (EAPOL). There are three components for 802.1X: • The Supplicant—This is the device connected to the switch. The device may be connected directly to the switch or via a point-to-point LAN segment. Typically the supplicant is a PC. • The Authenticator Port Access Entity (PAE)—This entity requires authentication from the supplicant. The authenticator is connected to the supplicant directly or via a point-to-point LAN segment. The OmniSwitch acts as the authenticator. • The Authentication Server—This component provides the authentication service and verifies the credentials (username, password, challenge, etc.) of the supplicant. On the OmniSwitch, only RADIUS servers are currently supported for 802.1X authentication. *Note: **IEEE 802.1x Multi-client and Multi-VLAN feature p**rovides the capability to force every user behind a given port to authenticate and be placed into their own applicable VLAN and allows multiple VLANs to be properly established on a single port. **In other words, multiple supplicants can be authenticated on a given 802.1x port***

802.1X enhancements on the OmniSwitch 6850 (Synonymous with the feature titled "Alcatel Access Guardian support") Note: The Alcatel Access Guardian is supported in Release 6.1.2r02 and in 6.1.2r03.	**Note:** the implementation of 802.1x on the OmniSwitch 6850 as described below is also synonymous with the feature titled "Alcatel Access Guardian support": In addition to the authentication and VLAN classification of 802.1x clients (supplicants), the OmniSwitch 6850 implementation of 802.1x secure port access extends this type of functionality to non-802.1x clients (non-supplicants). To this end device classification policies are introduced to handle both supplicant and non-supplicant access to 802.1x ports. By default non-supplicant devices are automatically blocked on 802.1x-enabled ports. In some cases, however, it is desirable to allow non-supplicant access on these ports. For example, using device policies a non-supplicant may gain access to a pre-determined VLAN. Such a VLAN might serve as a guest VLAN for such devices requiring restricted access to the switch. Supplicant devices are initially processed using 802.1x authentication via a remote RADIUS server. If authentication is successful and returns a VLAN ID, the supplicant is assigned to that VLAN. If not, then any configured device classification policies for the port are applied to determine VLAN assignment for the supplicant. If there are no policies, then the default port behavior for 802.1x ports is in affect. The following types of device classification policies are available: 1. 802.1x authentication—performs 802.1x authentication via a remote RADIUS server. 2. MAC authentications—performs MAC based authentication via a remote RADIUS server. 3. Group Mobility rules—uses Group Mobility rules to determine the VLAN assignment for a device 4. Strict Group Mobility rules—uses Group Mobility rules to determine the VLAN assignment for a device; does not allow assignment to authenticated VLANs. 5. VLAN ID—assigns the device to the specified VLAN. 6. Strict VLAN ID—assigns the device to the specified VLAN; does not allow assignment to authenticated VLANs. 7. Default VLAN—assigns a device to the default VLAN for the 802.1x port. 8. Strict Default VLAN—assigns a device to the default VLAN for the 802.1x port; does not allow assignment to authenticated VLANs. 9. Block—blocks a device from accessing the 802.1x port.
Alcatel Access Guardian support Note: The Alcatel Access Guardian is supported in Release 6.1.2r02 and in 6.1.2r03.	❑ Alcatel Access Guardian Support entails a set of security features that provide: o Automatic detection of 802.1x and non-802.1x devices o Flexible per port configuration of securities policies o 802.1x is used for user authentication, MAC-based authentication can be used for non-802.1x clients o Supported policies: ▪ Group Mobility rules ▪ Guest VLANs ▪ Default VLAN ▪ Block o Centralized location for user/device authentication-using RADIUS o Separate security policies can be configured for supplicants and non-supplicants ❑ Benefits: o Allows for flexible networks configuration which strengthens the security o Centralized management of users and devices reduces the administration cost ▪ All known users and devices are authenticated using RADIUS ▪ Change in one place only, takes effect everywhere in the network ▪ A mobile user will authenticate the same way a "wired" user o Guest users are placed in guest VLAN ❑ Applications: o Educational sector
Port Mapping • Allows traffic segregation at L2 • User ports in the same session cannot talk to each other **Note:** this feature is part of "Residential bridging features"	Port Mapping is a security feature, which controls communication between peer users. Each session comprises a session ID, a set of user ports, and/or a set of network ports. The user ports within a session cannot communicate with each other and can only communicate via network ports. In a port mapping session with user port set A and network port set B, the ports in set A can only communicate with the ports in set B. If set B is empty, the ports in set A can communicate with rest of the ports in the system. A port mapping session can be configured in the unidirectional or bi-directional mode. In the unidirectional mode, the network ports can communicate with each other within the session. In the bi-directional mode, the network ports cannot communicate with each other. Network ports of a unidirectional port mapping session can be shared with other unidirectional sessions, but cannot be shared with any sessions configured in the bi-directional mode. Network ports of different sessions can communicate with each other. **Port Mapping Specifications:** Ports Supported: Ethernet (10 Mbps)/Fast Ethernet (100 Mbps)/Gigabit Ethernet (1 Gb/1000 Mbps) /10 Gigabit Ethernet (10 Gb/10000 Mbps). Mapping Sessions: Eight sessions supported per standalone switch and stack. **Port Mapping Defaults:** Mapping Session: Creation: No mapping sessions Mapping Status configuration: Disabled Port Mapping Direction: Bi-directional

Access Control Lists (ACLs) Performance: Wire-speed ACLs are sometimes referred to as filtering lists.	Access Control Lists are Quality of Service policies used to control whether or not packets are allowed or denied at the switch or router interface. ACLs are distinguished by the kind of traffic they filter. In a QoS policy rule, the type of traffic is specified in the policy condition. The policy action determines whether the traffic is allowed or denied. In general, the types of ACLs include: • **Layer 2 ACLs**—for filtering traffic at the MAC layer. Usually uses MAC addresses or MAC groups for filtering. Layer 2 filtering filters traffic at the MAC layer. Layer 2 filtering may be done for both bridged and routed packets. As MAC addresses are learned on the switch, QoS classifies the traffic based on: • MAC address or MAC group • Source VLAN • Physical slot/port or port group The switch classifies the MAC address as both source *and* destination. • **Layer 3/4 ACLs**—for filtering traffic at the network layer. Typically uses IP addresses or IP ports for filtering. The QoS software in the switch filters routed and bridged traffic at Layer 3. For Layer 3/4 filtering, the QoS software in the switch classifies traffic based on: • Source IP address or source network group • Destination IP address or destination network group • IP protocol • Source TCP/UDP port • Destination TCP/UDP port or service or service group • Destination slot/port or destination port group • **Multicast ACLs**—for filtering IGMP traffic Multicast filtering may be set up to filter clients requesting group membership via the Internet Group Management Protocol (IGMP). IGMP is used to track multicast group membership. The IP Multicast Switching (IPMS) function in the switch optimizes the delivery of IP multicast traffic by sending packets only to those stations that request it. Potential multicast group members may be filtered out so that IPMS does not send multicast packets to those stations. Multicast traffic has its own global disposition. By default, the global disposition is accept. For multicast filtering, the switch classifies traffic based on the multicast IP address or multicast network group and any destination parameters. **ACL Specifications:** Maximum number of policy rules: 1024 Maximum number of policy rules per Ethernet port: 101 Maximum number of policy rules per 10-Gigabit Ethernet port: 997 Maximum number of policy conditions: 2048 Maximum number of policy actions: 2048 Maximum number of policy services: 256 Maximum number of groups (Network, MAC, service, port): 1024 Maximum number of group entries: 512 per group The following additional ACL features are available for improving network security and preventing malicious activity on the network: • **UserPorts**—A port group that identifies its members as user ports to prevent spoofed IP traffic. When a port is configured as a member of this group, packets received on the port are dropped if they Contain a source IP network address that does not match the IP subnet for the port. • **DropServices**—A service group that improves the performance of ACLs that are intended to deny packets destined for specific TCP/UDP ports. Using the DropServices group for this function minimizes processing overhead, which otherwise could lead to a DoS condition for other applications trying to use the switch. • **ICMP drop rules**—Allows condition combinations in policies that will prevent user pings, Thus reducing DoS exposure from pings. Two condition parameters are also available to provide more granular filtering of ICMP packets: icmptype and icmpcode. See "Configuring ICMP Drop Rules" in the network configuration Guide. • **BPDUShutdownPorts (Close user ports upon receipt of BPDU)**—A port group that identifies its members as ports that should not receive BPDUs. If a BPDU is received on one of these ports, The port is administratively disabled. In other words, this allows network administrators to prevent the connection of devices that can support bridging functionality to ports designated as user ports. See "Configuring a BPDUShutdownPorts Group" in the network configuration Guide. • **TCP connection rules—**Allows the determination of an established TCP connection by examining TCP flags found in the TCP header of the packet. Two condition parameters are available for defining a TCP connection ACL: established and tcpflags. See "Configuring a BPDUShutdownPorts Group" in the network configuration Guide. • **Early ARP discard—**ARP packets destined for other hosts are discarded to reduce processing overhead and exposure to ARP DoS attacks. No configuration is required to use this feature; It is always available and active on the switch. *Note that ARPs intended for use by a local subnet, AVLA! VRRP, and Local Proxy ARP are not discarded.*

Access Control List Manager (ACLMAN)	Access Control List Manager (ACLMAN) is a function of the Quality of Service (QoS) application that provides an interactive shell for using common industry syntax to create ACLs. Commands entered using the ACLMAN shell are interpreted and converted to Alcatel CLI syntax that is used for creating QoS filtering policies. This implementation of ACLMAN also provides the following features: • Importing of text files that contain common industry ACL syntax • Support for both standard and extended ACLs • Creating ACLs on a single command line • The ability to assign a name, instead of a number, to an ACL or a group of ACL entries • Sequence numbers for named ACL statements • Modifying specific ACL entries without having to enter the entire ACL each time to make a change • The ability to add and display ACL comments • ACL logging extensions to display Layer 2 through 4 packet information associated with an ACL **ACLMAN Overview:** ACLMAN is a function of the Alcatel QoS system that allows network administrators to configure and manage ACLs using common industry syntax. ACLs configured using ACLMAN are transparently converted into Alcatel QoS filtering policies and applied to the switch. An ACLMAN interactive shell provides an ACL command line interface that is similar to command interfaces that are available on other industry platforms. This shell serves as a configuration tool for creating ACLs using common industry syntax commands and/or importing industry syntax from text files. The following industry ACL types and features are supported with this implementation of ACLMAN: • Standard ACL. This type of ACL compares the source address of a packet to the source address specified in the ACL. • Extended ACL. This type of ACL compares the source and destination address of a packet to the source and destination address specified in the ACL. Also provides additional criteria for filtering packets. • Numbered ACL. This type of ACL refers to standard or extended ACLs that are assigned a number for identification. • Named ACL. This type of ACL refers to standard or extended ACLs that are assigned a name for identification. The following industry ACL types are currently not supported: • Reflexive ACLs • Context-Based Access Control • Authentication Proxy • Lock and Key (Dynamic ACLs) ACMAN Defaults: **ACLMAN Defaults:** ACL Disposition: Deny Logging rate time interval: 30 seconds

Distributed Intelligence

The AOS OmniSwitch product family has been designed to bring intelligence to an Enterprise network by implementing a host of intelligent features and services. Carrier-class intelligence insures that users and applications receive the priority and performance they need with ease-of-use management that extends across the entire enterprise. The OS6850 provides the necessary hardware queues, intelligence and granularity to properly identify, mark and prioritize data flows ensuring mission critical applications running smoothly.
The following is only a highlight of the state-of-the-art intelligent features supported by the OmniSwitch 6850 Series:

- VLAN Support:
  - 1024 VLANs, and 4,094 VLAN tags value support **4.3.12**
  - Per port, 802.1Q and policy based VLAN including authentication VLAN (A-VLAN) **4.1.11**
- Residential bridging features: DHCP option-82, DHCP-Snooping and Port Mapping
- Quality of Service
  - IEEE 802.1p, ToS, DSCP marking **4.1.8, 4.1.9**
  - QoS mapping: 802.1p to 802.1p & ToS & DSCP, ToS to ToS & 802.1p & DSCP, DSCP to DSCP & 802.1p & ToS
  - Classification per port, 802.1p(CoS) value, MAC SA/DA, TOS precedence, DSCP value, IP SA/DA, TCP/UDP port range
  - 8 egress queues per port to support strict and hybrid queuing (strict + weighted round robin queuing algorithm).
  - Ingress bandwidth rate limiting per port/flow in 64k increments
  - Egress bandwidth rate limiting per port in 1Mbps increments
- Routing Protocols
  - IPv4 & IPv6, RIPv1/v2 & OSPF & OSPF-ECMP & BGP & VRRP & PIM-SMv2 & & PIM-SSM & DVMRPv3 **4.3.10**

VLANs	In a flat-bridged network, a broadcast domain is confined to a single LAN segment or even a specific physical location, such as a department or building floor. In a switch-based network, such as one comprised of Alcatel-Lucent switching systems, a broadcast domain—or *VLAN*— can span multiple physical switches and can include ports from a variety of media types. For example, a single VLAN could span three different switches located in different buildings and include 10/100 Ethernet, Gigabit

	Ethernet, 802.1q tagged ports and/or a link aggregate of ports. Initially all switch ports are non-mobile and are assigned to VLAN 1. When additional VLANs are created on the switch, ports are assigned to the VLANs so that traffic from devices connected to these ports is bridged within the VLAN domain. Switch ports are either statically or dynamically assigned to VLANs. Static port assignment applies to both mobile and non-mobile (fixed) ports. Fixed ports are also statically assigned to *secondary* VLANs by defining 802.1Q tagged VLANs for the port. In addition, ports can belong to a link aggregate of ports. Dynamic assignment applies only to mobile ports and requires the additional configuration of VLAN rules. When traffic is received on a mobile port, the packets are examined to determine if their content matches any VLAN rules configured on the switch. Rules are defined by specifying a port, MAC address, protocol, network address, binding, or DHCP criteria to capture certain types of network device traffic. It is also possible to define multiple rules for the same VLAN. A mobile port is assigned to a VLAN if its traffic matches any one VLAN rule. **VLAN Specifications:** RFCs supported: 2674 – Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions. IEEE Standards supported: 802.1Q and 802.1D Maximum VLANs: 1024 (including VLAN#1) Maximum VLAN port associations: 32,768 Maximum IP router port VLANs: 1024 Maximum IPX router port VLANs: 1024 Maximum Spanning Tree VLANs: 254 Maximum Authenticated VLANs: 128 Maximum Router Mode Supported: Single The following provides a list of various types of VLAN rules supported. Rule Types: • DHCP o DHCP MAC & DHCP MAC Range o DHCP Port o DHCP Generic • Binding o MAC + IP+ Port o MAC + Port o Port + Protocol • MAC o MAC address & MAC Address Range • Mobile Tag • Network address o IP (IP Subnet) & IPX (IPX Network) • Protocol [including IP, IPv6, ARP, RARP, IPX (0x8137, 0xFFFF, 0xE0E0), AppleTalk (0x809b, 0x80F3) and DECNet] • Port
Rule Precedence	▪ DHCP Mac & DHCP Mac Range ▪ DHCP Port ▪ DHCP Generic ▪ Mac-Port-IP Binding ▪ Mac-Port Binding ▪ Port-Protocol Binding ▪ Mac & Mac Range ▪ IP Subnet ▪ IPX Network ▪ Protocol (Group Mobility classifies IPv6 frames)
Default VLAN	Every switch port, mobile or non-mobile, has a configured default VLAN. Initially, this is VLAN 1 for all ports, but is configurable using the **vlan port default** command.
Secondary VLANs	All mobile ports start out with a configured default VLAN assignment. When mobile port traffic matches VLAN criteria, the port is assigned to that VLAN. Secondary VLANs are any VLAN a port is subsequently assigned to that is not the configured default VLAN for that port. A mobile port can obtain more than one secondary VLAN assignment under the following conditions: • Mobile port receives untagged frames that contain information that matches rules on more than one VLAN. For example, if a mobile port receives IP and IPX frames and their is an IP protocol rule on VLAN 10 and an IPX protocol rule on VLAN 20, the mobile port is dynamically assigned to both VLANs. VLANs 10 and 20 become secondary VLAN assignments for the mobile port. • Mobile port receives 802.1Q tagged frames that contain a VLAN ID that matches a VLAN that has VLAN mobile tagging enabled. For example, if a mobile port receives frames tagged for VLAN 10, 20 and 30 and these VLANs have mobile tagging enabled, the mobile port is dynamically assigned to all three VLANs. VLANs 10, 20, and 30 become secondary VLAN assignments for the mobile port.
Automatic VLAN Containment (AVC)	When enabled, AVC prevents a port that has no VLANs mapped to an 802.1S Multiple Spanning Tree Instance (MSTI) from becoming the root port for that instance. Such ports are automatically assigned an infinite path cost value to make them an inferior choice for root port.

IP Virtual Router Port	A VLAN is available for routing traffic when a virtual router port is defined for that VLAN and at least one active port has joined the VLAN. If a VLAN does not have a router defined, its ports are in essence fire walled from other VLANs. Each VLAN supports one IP virtual router port and a maximum of 1024 IP router port VLANs are allowed per switch.
MAC Router Mode **Single MAC Router Mode ONLY**	The OmniSwitch 6850 operates only in single MAC router mode. In this mode, each router port VLAN is assigned the same MAC address, which is the base chassis MAC address for the switch. As a result, up to 1024 IP router port VLANs are supported per single switch. This also eliminates the need to allocate additional MAC addresses if more than 32 router port VLANs are defined.
IEEE 802.1Q	Alcatel-Lucent's 802.1Q is an IEEE standard for sending frames through the network tagged with VLAN identification. 802.1Q tagging can be configured and monitored on a single port in a switch or a link aggregation group in a switch. 802.1Q tagging is the IEEE version of VLANs. It is a method for segregating areas of a network into distinct VLANs. By attaching a label, or tag, to a packet, the packet can be identified as being from a specific area or identified as being destined for a specific area. When enabling a tagged port, you will also need to specify whether only 802.1Q tagged traffic is allowed on the port, or whether the port accepts both tagged and untagged traffic. "Tagged" refers to four bytes of reserved space in the header of the packet. The four bytes of "tagging" are broken down as follows: the first two bytes indicate whether the packet is an 802.1Q packet, and the next two bytes carry the VLAN identification (VID) and priority. On the ingress side, packets are classified in a VLAN. After classifying a packet, the switch adds an 802.1Q header to the packet. Egress processing of packets is done by the switch hardware. Packets have an 802.1Q tag, which may be stripped off based on 802.1Q tagging/stripping rules. If a port is configured to be a tagged port, then all the untagged traffic (including priority tagged, or VLAN 0 traffic) received on the port will be dropped. You do not need to reboot the switch after changing the configuration parameters. Priority tagged traffic, or traffic from VLAN 0, is used for Quality of Service (QoS) functionality. 802.1Q views priority tagged traffic as untagged traffic. Mobile ports can be configured to accept 802.1Q traffic by enabling the VLAN mobile tagging feature. The port can be assigned to as many 802.1Q VLANs as necessary, up to 4093 per port or 32768 VLAN port associations. For the purposes of Quality of Service (QoS), 802.1Q ports are always considered to be *trusted* ports. 802.1Q tagging is done at wire speed, providing high-performance throughput of tagged frames. **IEEE 802.1Q Specifications:** IEEE Specification: Draft Standard P802.1Q/D11 IEEE Standards for Local And Metropolitan Area Network: Virtual Bridged Local Area Networks, July 30, 1998 Maximum Number of Tagged VLANs per Port: 4093 Maximum Number of Untagged VLANs per Port: one untagged VLAN per port Maximum Number of VLAN Port Associations: 32768 What type of frames accepted: Both tagged and untagged frames are accepted
Basic IP Routing	Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing and control information that allow packets to be forwarded on a network. IP is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP is associated with several Layer 3 and Layer 4 protocols. These protocols are built into the base code loaded on the switch and they include: • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP) • Bootstrap Protocol (BOOTP)/Dynamic Host Configuration Protocol (DHCP) • Simple Network Management Protocol (SNMP) • Telnet • File Transfer Protocol (FTP) / Secure FTP • Address Resolution Protocol (ARP) • Internet Control Message Protocol (ICMP) • RIP I / RIP II The base IP software allows one to configure an IP router port, static routes, a default route, the Address Resolution Protocol (ARP), the router primary address, the router ID, the Time-to-Live (TTL) Value, IP-directed broadcasts, and the Internet Control Message Protocol (ICMP). In addition, this software allows one to trace IP route, display Transmission Control Protocol (TCP) information, and display User Data-gram Protocol (UDP) information.
Routing Protocols	IP is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be forwarded. IP is documented in RFC 791 and is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP is enabled on the switch by default. Static IP Routing is supported. Dynamic IP Routing support: VRRP, RIPv1, RIPv2, and OSPFv2 Router Discover Protocol (RDP): The Router Discovery Protocol (RDP) is an extension of ICMP that allows end hosts to discover routers on their networks. This implementation of RDP supports the router requirements as defined in RFC 1256. **L3 Routing Protocols (IPv4)** **IP Routing**

	• Static routing • RIP v1 & v2 • OSPF v2 • BGP v4 **Multicast** • IGMP v1, v2 & v3 snooping • PIM-SM • PIM-DM **(Future Release)** • DVMRP **Network Protocol** • TCP/IP stack • ARP • DHCP relay **4.1.5** • Generic UDP relay per VLAN **Resilience** • VRRP v2 **L3 Routing Protocols (IPv6)** IP Routing • Static routing • RIP ng • OSPF v3 **Multicast** • MLD snooping • PIM-SM • PIM-DM **(Future Release)** **Network Protocol** • TCP/IP stack • DHCP relay (including generic UDP relay) • ARP **Resilience** • VRRPv3 **(Future Release)** **Layer-3 Routing (IPX)** IPX Routing • Static routing • RIP/SAP
The Virtual Router Redundancy Protocol (VRRP)	The Virtual Router Redundancy Protocol (VRRP) is a standard router redundancy protocol supported in IP version 4. It is based on RFC 2338 and provides redundancy by eliminating the single point of failure inherent in a default route environment. VRRP allows routers on a LAN to back up a default route. VRRP dynamically assigns responsibility for a virtual router to a physical router (VRRP router) on the LAN. The virtual router is associated with an IP address (or set of IP addresses) on the LAN. A virtual router master is elected to forward packets for the virtual router's IP address. If the master router becomes unavailable, the highest priority backup router will transition to the master state. In addition, VRRP Tracking is also supported. A virtual router's priority may be conditionally modified to prevent another router from taking over as master. Tracking policies are used to conditionally modify the priority setting whenever a VLAN, slot/port, and/or IP address associated with a virtual router goes down. **VRRP Specifications:** RFCs Supported: ▪ RFC 2338–Virtual Router Redundancy Protocol ▪ RFC 2787–Definitions of Managed Objects for the Virtual Router Redundancy Protocol Compatible with HSRP: No Maximum number of virtual router instances: 255 *(A virtual router is defined by a virtual router identifier (VRID) and a set of associated IP addresses on the LAN)* Maximum number of IP addresses: 1 for the IP address owner; more than 1 address may be configured if the router is a backup for a master router that supports multiple addresses
IGMP	IGMP is used by IPv4 systems (hosts and routers) to report their IP multicast group memberships to any neighboring multicast routers. IGMP version 2 (IGMPv2) handles forwarding by IP multicast destination address only. IGMP version 3 (IGMPv3) handles forwarding by source IP address and IP multicast destination address. OmniSwitch 6850 Series switches support IGMPv2 and IGMPv3. In IGMPv2, each membership report contains only one multicast group. In IGMPv3, membership reports contain many multicast groups up to the Maximum Transmission Unit (MTU) size of the interface. IGMPv3 uses source filtering and reports multicast memberships to neighboring routers by sending membership reports. IGMPv3 also supports Source Specific Multicast (SSM) by allowing hosts to report interest in receiving packets only from specific source addresses or from all but specific source addresses. **Note.** It should be noted that in the current release SSM packet forwarding is not done between ports in

	the same VLAN. However, SSM forwarding between different VLANs (routing) is supported. In addition, the current implementation of IGMPv3 and SSM only forwards packets to a list of included sources for a given multicast destination. Exclude list forwarding is not supported, as it is not a requirement for SSM, and specifically Protocol Independent Multicast–Source Specific Multicast (PIM-SSM).
IP Multicast Switching and Routing (IPMSR)	IP multicast routing can be used for IP Multicast Switching and Routing (IPMSR). IP multicast routing is a way of controlling multicast traffic across networks. The IP multicast router discovers which networks want to receive multicast traffic by sending out Internet Group Management Protocol (IGMP) queries and receiving IGMP reports from attached networks. The IGMP reports signal that users want to join a multicast group. The IPv6 multicast router discovers multicast listeners by sending out Multicast Listener Discovery (MLD) Protocol queries and receiving MLD reports from attached networks. The MLD reports signal that users want to join a IPv6 multicast group. If there is more than one IP multicast router in the network, the router with the lowest IP address is elected as the querier router, which is responsible for querying the sub-network for group members. The IP multicast routing package provides the following two separate protocols: • Protocol Independent Multicast — Sparse Mode (PIM-SM) and Dense Mode (PIM-DM) • Distance Vector Multicast Routing Protocol (DVMRP) The multicast routing protocols build and maintain a multicast routing database. The multicast routing protocols forward multicast traffic to networks that have requested group membership to a specific multicast group. IPMS uses decisions made by the routing protocols and forwards multicast traffic to ports that request group membership.
Multicast Address Boundaries	Multicast boundaries confine scoped multicast addresses to a particular domain. Confining scoped addresses helps to ensure that multicast traffic passed within a multicast domain does not conflict with multicast users outside the domain. **Multicast Boundary Specifications:** RFCs Supported: 2365—Administratively Scoped IP Multicast 2932—IPv4 Multicast Routing MIB Maximum Multicast Flows per switch: 400 (with hardware routing; see note below) Valid Scoped Address Range: 239.0.0.0 to 239.255.255.255 ***Note.*** *If software routing is used, the number of total flows supported is variable, depending on the number of flows and the number of routes per flow.*
Multicast Routing	The OmniSwitch 6850 Series supports multicast routing and includes configuration options for multicast address boundaries, the Distance Vector Multicast Routing Protocol (DVMRP), and Protocol-Independent Multicast (PIM). Multicast traffic consists of a data stream that originates from a single source and is sent to hosts that have subscribed to that stream. Live video broadcasts; video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news services are examples of multicast traffic. Multicast traffic is distinguished from unicast traffic and broadcast traffic. Multicast boundaries confine scoped multicast addresses to a particular domain. Confining scoped addresses helps to ensure that multicast traffic passed within a multicast domain does not conflict with multicast users outside the domain. Distance Vector Multicast Routing Protocol (DVMRP) is a dense-mode multicast routing protocol designed to assist routers in propagating IP multicast traffic through a network. DVMRP works by building per-source broadcast trees based on routing exchanges, then dynamically creating per-source, group multicast delivery trees by pruning the source's truncated broadcast tree.
Diagnosing Switch Problems	
Several tools are available for diagnosing problems that may occur with the switch. These tools include: • Port Mirroring • Port Monitoring • Remote Monitoring (RMON) probes • Switch Health Monitoring • SFlow • Monitoring Memory tools • Switch Logging Port mirroring copies all incoming and outgoing traffic from a single mirrored Ethernet port to a second mirroring Ethernet port, where it can be monitored with a Remote Network Monitoring (RMON) probe or network analysis device without disrupting traffic flow on the mirrored port. Switch Health monitoring software checks previously configured threshold levels for the switch's consumable resources, and notifies the Network Monitoring Station (NMS) if those limits are violated.	
Port Mirroring	Ethernet ports supporting port mirroring include 10BaseT/100BaseTX/1000BaseT (RJ-45), 1000BaseSX/LX/LH, and 10GBaseS/L (LC) connectors. When port mirroring is enabled, the active "mirrored" port transmits and receives network traffic normally, and the "mirroring" port receives a copy of all transmit and receive traffic to the active port. You can connect an RMON probe or network analysis device to the mirroring port to see an exact duplication of traffic on the mirrored port without disrupting network traffic to and from the mirrored port. Port mirroring runs in the Chassis Management software and is supported for Ethernet (10 Mbps), Fast

	Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps), and 10 Gigabit Ethernet (10000 Mbps) ports. One (1) port mirroring session is supported in a standalone switch. OmniSwitch 6850 Family switches support "N-to-1" port mirroring where up to 24 source ports can be mirrored to a single destination port. By default, port-mirroring sessions are bi-directional. OmniSwitch 6850 Series switches support mirroring between any 10/100/1000Mbps port to any other 10/100/1000Mbps port and between any fiber MiniGBIC SFP to any other fiber MiniGBIC SFP port. **Port Mirroring Specifications:** • Ports Supported: Ethernet (10Mbps)/Fast Ethernet (100Mbps)/Gigabit Ethernet and 10-Gigabit Ethernet • Mirroring Sessions Supported: One session supported per standalone switch. • N-to-1 Mirroring supported: Up to 24 source ports can be mirrored to a destination port. • Port Capacity Requirements: Mirrored (monitored) and mirroring (monitoring) ports must be of identical capacity (both ports support identical speeds) or the Mirroring port must be of higher capacity than the mirrored port. (Example: A mirrored Fast Ethernet port supports 100 Mbps, while a Mirroring Gigabit Ethernet port supports 1000 Mbps). • Range of Unblocked VLAN Ids: 1 to 4094.
Port Monitoring	Port Monitoring – Port monitoring provides the ability to capture a packet trace locally for real time display or for replay later through a packet analyzer to determine network issues. It works like port mirroring but instead of sending the captured packets to another port, it stores these packets to a local file for later retrieval or display. **Port Monitoring Specifications:** • Ports Supported: Ethernet (10 Mbps) / Fast Ethernet (100 Mbps) / Gigabit Ethernet • Monitoring Sessions Supported: one per switch • File Type Supported: ENC file format (Network General Sniffer Network Analyzer Format) By default, a port monitoring session will never be disabled. The length of time before a port monitoring session is disabled is from 0 (the default, where the session is permanent) to 2147483647 seconds. By default, a file called pmonitor.enc is created in the /flash directory when you configure and enable a port monitoring session. By default, port-monitoring sessions are bi-directional. The port-monitoring feature allows you to examine packets to and from a specific Ethernet port. Port monitoring has the following features: • Software commands to enable and display captured port data. • Captures data in Network General® file format. • A file called pmonitor.enc is created in /flash memory when you configure and enable a port monitoring session. • Data packets time stamped. • One port monitored at a time. • RAM-based file system. • Statistics gathering and display The port-monitoring feature also has the following restrictions: • Estimated packet capture rate is around 500 packets/second. • The maximum number of monitoring session is limited one per chassis • Link Aggregation ports can not be monitored • If both mirroring and monitoring are enabled then packets will be either mirrored or monitored (i.e., sent to CPU), whichever comes first. You can select to dump real-time packets to a file. Once a file is captured, you can FTP it to a Sniffer or PC for viewing: The port-monitoring feature allows you to examine packets to and from a specific Ethernet port (either ingress or egress). You can select to dump captured data to a file, which can be up to 140 K. Once a file is captured, you can FTP it to a Protocol Analyzer or PC for viewing. The OmniSwitch 6850 supports one session per switch. By default, the switch will create a data file called "pmonitor.enc" in flash memory. When the 140 K limit is reached the switch will begin overwriting the data starting with the oldest captured data. However, you can configure the switch so it will not overwrite the data file. In addition, you can configure additional port monitoring files as long as you have enough room in flash memory.

SSHv2 **4.1.2** SSHv2 for secure CLI session with PKI is also supported	The OmniSwitch Secure Shell feature provides a secure mechanism that allows you to log in to a remote switch, to execute commands on a remote device, and to move files from one device to another. Secure Shell provides secure, encrypted communications even when your transmission is between two untrusted hosts or over an un-secure network. The OmniSwitch includes both client and server components of the Secure Shell interface and the Secure Shell FTP file transfer protocol. SFTP is a subsystem of the Secure Shell protocol. All Secure Shell FTP data are encrypted through a Secure Shell channel. Secure Shell protects against a variety of security risks including the following: • IP spoofing • IP source routing • DNS spoofing • Interception of clear-text passwords and other data by intermediate hosts • Manipulation of data by users on intermediate hosts *Note. The OmniSwitch supports Secure Shell Version 2 only.* Algorithm and key Exchange: One or several host-specific DSA keys identify the OmniSwitch Secure Shell server. Both the client and server process the key exchange to choose a common algorithm for encryption, signature, and compression. This key exchange is included in the Secure Shell transport layer protocol. It uses a key agreement to produce a shared secret that cannot be determined by either the client or the server alone. The key exchange is combined with a signature and the host key to provide host authentication. Once the exchange is completed, the client and the server turn encryption on using the selected algorithm and key. The following elements are supported: Host key Type: DSA Cipher Algorithms; AES, Blowfish, Cast, 3DES, Arcfour, and Rijndael Signature Algorithms: MD5, and SHA1 Compression Algorithms: None-supported Key Exchange Algorithms: ▪ Diffie-hellman-group-exchange-shal ▪ Diffie-hellman-group1-shal When used as an SSH Server, the following SSH Software is supported: OpenSSH: Sun Solaris, Win NT + Cygwin, Mac OSX, Linux Red Hat F-Secure: Sun Solaris, Win 2000, Win NT, Win XP, Mac OS9 SSH-Communication: Sun Solaris, Win 2000, Win NT, Win XP, Linux Red Hat PuTTY: Win 2000, Win NT, Win XP, Mac OS9 MAC-SSH: Mac OS9, Mac OSX When used as an SSH Client, the following SSH Software is supported: OpenSSH: Sun Solaris, Win NT + Cygwin, Linux Red Hat, AOS F-Secure: Sun Solaris, Win 2000, Win NT SSH-Communication: Sun Solaris, Win 2000, Win NT, Win XP, Linux Red Hat

OmniSwitch 6850 Series – IETF / IEEE Standards

The OmniSwitch 6850 Series is fully compliant with the relevant industry standards to include the following:
For further references on these Standards, refer to: www.IEEE.com
For further references on these Standards, refer to: www.IETF.org

IEEE	
IEEE 802.1D-1998	STP - Bridging (Media Access Control Bridges)
IEEE 802.1p	CoS/QoS
IEEE 802.1Q	VLANs - Virtual Bridged local Area Networks Draft Standard P802.1Q/D11 IEEE Standards for Local And Metropolitan Area Network: Virtual Bridged Local Area Networks, July 30, 1998
IEEE 802.1s	MSTP - Multiple VLAN Spanning Tree
IEEE 802.1x	Security - Port-based Network Access (supplement to 802.1D)
Extended 802.1x	Authenticated VLAN (multiple MAC, multiple VLANs per port)
IEEE 802.1x MIB – Port Access	IEEE 802.1x MIB – Port Access is supported.
IEEE 802.1v	Protocol VLANs
IEEE 802.1w	RSTP - Rapid reconfiguration
IEEE 802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
IEEE 802.3i	10BASE-T
IEEE 802.3ab	The IEEE 802.3ab standard describes the specifications for the 1000BASE-T twisted-pair GigEth.
IEEE 802.3ac	VLAN tagging
IEEE 802.3ad	Link Aggregation (Dynamic)
IEEE 802.3ae	10-Gigabit Ethernet
IEEE 802.3af	Power over Ethernet (PoE)
IEEE 802.3x	Ethernet flow control
IEEE 802.3u	The IEEE 802.3u standard describes the specification 100BASE-TX, & 100BASE-FX Ethernet
IEEE 802.3z	The IEEE 802.3z standard describes the specifications for the 1000BASE-X fiber optic Gigabit Eth.

Access Control Lists – ACLs 4.3.11

Access Control Lists (ACLs) are Quality of Service (QoS) policies used to control whether or not packets are allowed or denied at the switch or router interface. ACLs are sometimes referred to as filtering lists.
ACLs are distinguished by the kind of traffic they filter. In a QoS policy rule, the type of traffic is specified in the policy condition. The policy action determines whether the traffic is allowed or denied.
In general, the types of ACLs include:
• *Layer 2 ACLs*—for filtering traffic at the MAC layer. Usually uses MAC addresses or MAC groups for filtering.
• *Layer 3/4 ACLs*—for filtering traffic at the network layer. Typically uses IP addresses or IP ports for filtering;
• *Multicast ACLs*—for filtering IGMP traffic

ACL Specifications

These specifications are the same as those for QoS in general:

Maximum number of policy rules	1024
Maximum number of policy rules per Ethernet port	101
Maximum number of policy rules per 10Gigabit port	997
Maximum number of policy conditions	2048
Maximum number of policy actions	2048
Maximum number of policy services	256
Maximum number of groups (Network, MAC, service, port)	1024
Maximum number of group entries	512 per group

VLANs

In a flat-bridged network, a broadcast domain is confined to a single LAN segment or even a specific physical location, such as a department or building floor. In a switch-based network, such as one comprised of Alcatel-Lucent switching systems, a broadcast domain—or *VLAN*— can span multiple physical switches and can include ports from a variety of media types. For example, a single VLAN could span three different switches located in different buildings and include 10/100 Ethernet, Gigabit Ethernet, 802.1q tagged ports and/or a link aggregate of ports.

VLAN Specifications

RFCs Supported	**2674 - Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions**
IEEE Standards Supported	**802.1Q - Virtual Bridged Local Area Networks 802.1D - Media Access Control Bridges**
Maximum VLANs per switch	**1024 (including the default VLAN#1)**
Maximum VLAN port associations per switch	**32,768**
Maximum IP router port VLANs per switch	**1024 (single router MAC mode)**
Maximum IPX router port VLANs per switch	**256 (single router MAC mode)**
Maximum IP router interfaces per VLAN	**8**
Maximum Spanning Tree VLANs per switch	**253**
Maximum authenticated VLANs per switch	**128**
MAC Router Mode Supported	**Single**

Managing Authentication Servers

This section describes authentication servers and how they are used with the switch. The types of servers described include Remote Authentication Dial-In User Service (RADIUS), Lightweight Directory Access Protocol (LDAP), and SecurID's ACE/Server.

Authentication Server Specifications

RADIUS RFCs Supported	RFC 2865–Remote Authentication Dial In User Service (RADIUS) RFC 2866–RADIUS Accounting RFC 2867–RADIUS Accounting Modifications for Tunnel Protocol Support RFC 2868–RADIUS Attributes for Tunnel Protocol Support RFC 2809–Implementation of L2TP Compulsory Tunneling via RADIUS RFC 2869–RADIUS Extensions RFC 2548–Microsoft Vendor-specific RADIUS Attributes RFC 2882–Network Access Servers Requirements: Extended RADIUS Practices
LDAP RFCs Supported	RFC 1789–Connectionless Lightweight X.5000 Directory Access Protocol RFC 2247–Using Domains in LDAP/X.500 Distinguished Names RFC 2251–Lightweight Directory Access Protocol (v3) RFC 2252–Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions RFC 2253–Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names RFC 2254–The String Representation of LDAP Search Filters RFC 2256–A Summary of the X.500 (96) User Schema for Use with LDAPv3
Other RFCs	RFC 2574–User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) RFC 2924–Accounting Attributes and Record Formats RFC 2975–Introduction to Accounting Management RFC 2989–Criteria for Evaluating AAA Protocols for Network Access
Maximum number of authentication servers in single authority mode	4 (not including any backup servers)
Maximum number of authentication servers in multiple authority mode	4 per VLAN (not including any backup servers)
Maximum number of servers per Authenticated Switch Access type	4 (not including any backup servers)
CLI Command Prefix Recognition	The aaa radius-server and aaa ldap-server commands support prefix recognition.

Supported Protocols and Services

Supported TCP Service Parameters		
Bgp (179)	Gopher (70)	Pop3 (110)
Chargen (19)	Hostname (101)	Smtp (25)
Cmd (rcmd, 514)	Ident (113)	Sunrpc (111)
Daytime (13)	Irc (194)	Syslog (514)
Discard (9)	Klogin (543)	Tacacs (49)
Domain (53)	Kshell (544)	Talk (517)
Echo (7)	Login (rlogin, 513)	Telnet (23)
Exec (rsh, 512)	Lpd (515)	Time (37)
Finger (79)	Nntp (119)	Uucp (540)
Ftp (21)	Pim-auto-rp(496)	Whois (43)
Ftp-data (20)	Pop2 (109)	Www (HTTP, 80)

Supported UDP Service Parameters		
Biff (512)	Nameserver (obsolete, 42)	Snmptrap (162)
Bootpc (BOOTP) client (68)	netbios-dgm (138)	Sunrpc (111)
Bootps (BOOTP) server (67)	Netbios-ns (137)	Syslog (514)
Discard (9)	Netbios-ss (139)	Tacacs (49)
Dnsix (195)	Non500-isakmp (4500)	Talk (517)
Domain (DNS, 53)	Ntp (123)	Tftp (69)
Echo (7)	Pim-auto-rp (496)	Time (37)
Isakmp (500)	Rip (router, in.routed, 520)	Who (rwho, 513)
Mobile-ip (434)	Snmp (161)	Xdmcp (177)